THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, LLC, Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	)	Case No.: No. 2:18-cv-00094-EWH-LRL **PUBLIC VERSION - REDACTED**

PLAINTIFF CENTRIPETAL NETWORKS, LLC'S
PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Pursuant to the Court's March 7, 2023 Order (Dkt. No. 682), Centripetal Networks, LLC ("Centripetal") respectfully submits the following Proposed Findings of Fact and Conclusions of Law on the issues involved in the above-entitled case with respect to the Asserted Claims of U.S. Patent Nos. 9,686,193 ("the '193 Patent"), 9,203,806 ("the '806 Patent"), and 9,560,176 ("the '176 Patent"), (collectively "Asserted Patents"). To avoid duplicative findings, Centripetal incorporates the Joint Statement of Undisputed Issues and Stipulations (Dkt. No. 701) and the Joint Stipulation Regarding Not Recalling Parties' Damages Experts, including the exhibit marked PTX-1958 (Dkt. Nos. 699, 700).

PROPOSED FINDINGS OF FACT

I. FACTS ON THE PROCEDURAL BACKGROUND

1. On February 13, 2018, Centripetal filed the Complaint asserting that Defendant Cisco Systems, Inc. ("Cisco") infringes U.S. Patent No. 9,686,193; U.S. Patent No. 9,560,176; U.S. Patent No. 9,560,077 ("the '077 Patent"); U.S. Patent No. 9,413,722 ("the '722 Patent"); U.S. Patent No. 9,203,806; U.S. Patent No. 9,160,713 ("the '713 Patent"); U.S. Patent No. 9,124,552 ("the '552 Patent"); U.S. Patent No. 9,565,213 ("the '213 Patent"); U.S. Patent No. 9,137,205 ("the '205 Patent"); and U.S. Patent No. 9,674,148 ("the '148 Patent").

2. On March 29, 2018, Centripetal filed an Amended Complaint to add an assertion of infringement of U.S. Patent No. 9,917,856 ("the '856 Patent").

3. Cisco filed a number of petitions for *inter partes* review ("IPR") of some of the patents asserted against it and filed for a Motion to Stay Pending Resolution of IPR Proceedings. The Court granted the stay on February 25, 2019. Dkt. No. 58.

4. After Centripetal filed its Complaint, Cisco filed petitions for IPR of the Asserted Claims of the '176 Patent and '193 Patent.

5. Cisco did not file petitions for IPR of the '856 Patent and '806 Patent within one year of service of the Complaint.

6. The United States Patent and Trademark Office's Patent Trial & Appeal Board ("PTAB") denied the institution of IPRs of the Asserted Claims of the '176 Patent and '193 Patent over the prior art asserted by Cisco in its petitions.

7. On September 18, 2019, the Court issued an order lifting the stay in part with respect to patents and claims not currently subject to IPR proceedings, which were the '193, '806, '176, and '856 Patents. Dkt. No. 68.

8. The Court held a claim construction hearing on February 6, 2020 (Dkt. No. 189) and issued an order on claim construction on February 20, 2020 (Dkt. No. 202, the "Claim Construction Order").

9. The Court held a pretrial conference on April 23, 2020 (Dkt. No. 407) and issued a final pretrial order on April 23, 2020 (Dkt. No. 408). The Court issued an amended final pretrial order on April 27, 2020. Dkt. No. 411.

10. Centripetal is the owner of the '193, '806, '176, and '856 Patents (the "Asserted Patents").[1]

11. Centripetal is asserting that Cisco infringes Claims 18 and 19 of the '193 Patent, Claims 9 and 17 of the '806 Patent, and Claims 11 and 21 of the '176 Patent (the "Asserted Claims").

12. The Court held a bench trial from May 6, 2020 to June 11, 2020, with a final hearing relating to damages on June 25, 2020.

[1] On June 6, 2023, the Court stayed the proceedings with regard to the '856 Patent.

13. The Court issued an opinion and order pursuant to Federal Rule of Civil Procedure 52(a) on October 5, 2020 (Dkt. No. 621) finding willful infringement and validity, and awarding enhanced damages.

14. The Court issued an order on March 17, 2021 (Dkt. No. 638) denying Cisco's post-trial motions filed pursuant to Federal Rules of Civil Procedure 59(a)(2), 52(b), and 54(b).

15. Cisco appealed, and the Federal Circuit vacated the Court's orders (Dkt. Nos. 621, 638) based on a stock ownership issue, without reaching any substantive appealed issues. *See Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1040 (Fed. Cir. 2022), *cert. denied*, 143 S. Ct. 487 (2022). The Federal Circuit remanded this matter for resolution. *Id.*

16. This Court has proceeded under Federal Rule of Civil Procedure 63. *See* Dkt. No. 662.

17. The Court scheduled a hearing pursuant to Federal Rule of Civil Procedure 63 for June 22-23, and 26-27, 2023. Dkt. No. 682. Cisco requested the Court recall two fact witnesses pursuant to Federal Rule of Civil Procedure 63, which the Court granted. *Id.* The Court requested the parties each present a technology tutorial and argument, in addition to presenting the requested fact witness testimony. *Id.* After the Court's June 6, 2023 order staying the proceedings as to the '856 Patent, Cisco represented to the Court that it will only call one fact witness.

18. This Court hereby certifies familiarity with the complete record in this case.

II. FACTS RELATED TO THE PARTIES AND ACCUSED PRODUCTS

A. Centripetal Is an Innovator in Network Security

19. Centripetal is a limited liability company duly organized and existing under the laws of the State of Delaware, with its principal place of business in Reston, Virginia. Dkt. No. 673.

20. In 2009, decorated veteran Steven Rogers founded Centripetal as a start-up cybersecurity company to develop a new solution that leveraged threat intelligence to detect and proactively stop cybersecurity threats. Tr. 233:20-236:10; 308:14-309:24; 1202:23-1203:5.

21. Centripetal focused on using threat intelligence software and hardware to protect cyber networks. Tr. 235:23-25. Centripetal operated to solve cybersecurity problems in an ever-changing and developing industry using both inline and out-of-band methods. Tr. 239:6-15; see PTX-1591; DTX-1270.

22. Centripetal developed a product called RuleGATE that was first sold in December of 2014. Tr. 285:24-286:1. RuleGATE is a platform that was deployed to operationalize Cyber Threat Intelligence ("CTI") by taking the raw intelligence and applying it to network traffic. Tr. 311:2-14; PTX-1219.

23. RuleGATE reduces the surface area that can be attacked in a network by blocking traffic that should not be allowed. Tr. 312:3-313:20; PTX-957.

24. Centripetal's RuleGATE product practices the Asserted Patents in this case, which Cisco does not dispute. Tr. 1381:13-1385:19; PTX-1215. Centripetal marks its RuleGATE product with the patents that it practices. Tr. at 1203:12-1204:3, PTX-528; Tr. 1383:18-1385:19; PTX-1215; *see* Findings of Fact, Section III.

B. Cisco Is One of the World's Largest Networking Companies

25. Defendant Cisco is a Delaware corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134.

26. Cisco was founded in 1984 as a networking company. Cisco has dealt in network devices throughout its operation, selling including routers, switches, firewalls and other technologies. Cisco represents itself as the largest provider of network infrastructure and services in the world. PTX-576 at 991.

C. Cisco Approached Centripetal for its Patented Solutions and then Copied Centripetal's Technology

27. The parties had a history prior to this litigation, as described below.

28. Between 2015 and 2017, Cisco demonstrated an interest in Centripetal's innovative technology, as evidenced by the parties' numerous meetings and discussions about Centripetal's business, technology, products, and patents, including multiple product demonstrations. *See, e.g.*, Tr. 1018:4-16; 1019:8-18; 1020:23-1021:15; 1024:16-1026:18.

29. Cisco contacted Steven Rogers, Centripetal's CEO, in 2015 to learn about Centripetal's patented technology, which it viewed as a solution that "fit into the types of solutions [Cisco] needed for customers . . . that went beyond the offerings that Cisco had at the time." Tr. 256:8-257:12.

30. In 2015, Steven Rogers had a meeting with Pavan Reddy, a Cisco employee, where Mr. Rogers disclosed Centripetal's product offerings and the effectiveness of their solutions. Tr. 256:8-257:12. Mr. Reddy and Mr. Rogers had a follow-up meeting that same year, where Centripetal provided a demonstration of its system and explained why it was an effective method of cyber defense. Tr. 256:8-257:12.

31. As a result of these meetings, on January 26, 2016, Centripetal and Cisco entered into a nondisclosure agreement ("NDA"), requiring Cisco to keep Centripetal's confidential, proprietary or non-public information "strictly confidential" and "not use any Information in any manner . . . other than solely in connection with its consideration of" a possible partnership. Tr. 257:13-18, 258:13-19, 1213:16-20, 1214:3-20; PTX-99 (the NDA).

32. Centripetal and Cisco signed the NDA to explore jointly selling Centripetal's technology in Cisco products and/or a Cisco investment in Centripetal. Tr. 1213:16-20, 1214:3-20; PTX-99.

33. After Cisco executed the NDA, Centripetal and Cisco had several meetings, including with Cisco's technical and corporate development teams, where Centripetal provided multiple demonstrations of RuleGATE and disclosed information about its patented technology. PTX-547 at 389-92, 396; Tr. at 258:21-25, 260:2-18, 1219:22-1222:25, 1223:23-1224:22, 1225:11-1227:18 (discussing PTX-102).

34. On February 4, 2016, Centripetal presented information about its patented technology and products to Cisco in a WebEx meeting, including details of its patented technology covered by the Asserted Patents. Tr. 258:21-260:4, 1215:14-1216:6; 1220:9-1224:22; PTX-547 at 389-92, 396; PTX-102 at 001. For example, Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies 'automate workflow'" and how its "patented" "instant host correlation" conveys "real time analytics." PTX-547 at 389-91; Tr. 258:21-25, 260:2-18; 1220:1-1222:25.

35. During that meeting, Centripetal presented "detailed, highly sensitive, confidential and proprietary information about its patented technology and products," including its patented filter algorithms to prevent exfiltration ('193 Patent), correlation algorithms ('176 Patent), and Centripetal's patented technologies for rule swapping ('806 Patent) and for detecting threats in encrypted traffic. Tr. 1219:15-1224:22; PTX-547 at 389-91.

36. Centripetal also answered various questions about its patented technologies at the meeting. Tr. 1225:12-16, 1227:9-18; PTX-102 at 001.

37. The next day, on February 5, 2016, Centripetal's Jonathan Rogers sent an e-mail to Cisco summarizing the WebEx meeting, noting that Cisco "seemed to hone in on our filter technology and algorithms. The algorithms are a significant networking technology with broad

application that we've productized for security. There were also a few questions on our patents. . ." Tr. 1226:10-1227:18; PTX-102 at 001; PTX-1046.

38. On February 5, 2016, TK Keanini, a Cisco Distinguished Engineer who had attended the WebEx meeting, wrote an internal email to his team stating:

> It appears that most of their intellectual property lays in the claim that given 'n' amount of signatures (they call them rules) they are able to instrument them in an inline device. . . . What might be wor[th] exploration is to look at these algorithms they have and how general purpose they may be for data synthesis – high performance set theoretical functions. Again, knowing what patent offices will allow and not allow, I'd be very surprised if they were able to make claims on the algorithms themselves but we don't know until we study their claims.

PTX-134 at 3; *see also* Tr. 1128:8-1129:5; Tr. 2815:2-3.

39. Centripetal and Cisco had further follow-up meetings and communications after the February 2016 WebEx meeting, demonstrating Cisco's continued interest in Centripetal. Tr. 1233:20-1234:9.

40. For example, in July 2016, Cisco invited Centripetal to be a technology partner at its Cisco Live conference, where Centripetal again presented its patented solution. Tr. 1234:10-16, 1297:23-1298:24; *see also* Tr. 1024:16-25.

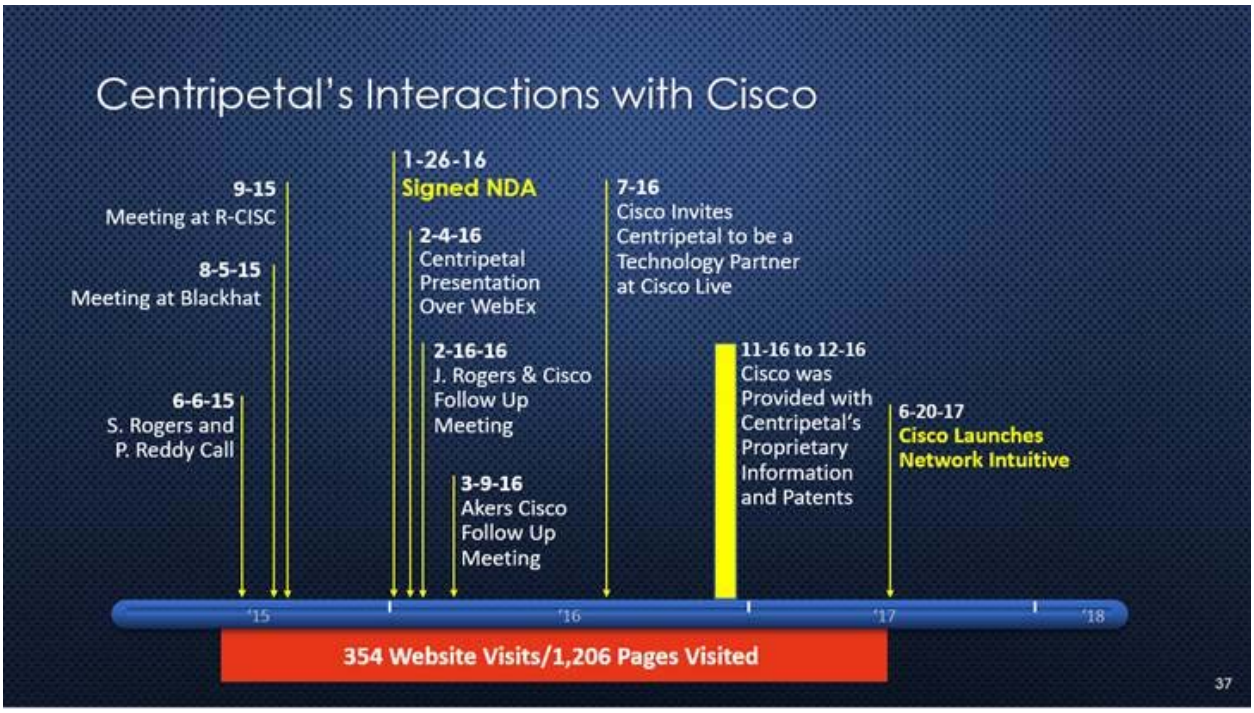
41. At the conference, Cisco's security architect, Joseph Muniz, demonstrated great interest in Centripetal's patented technology and requested a product demonstration. Tr. 1298:21-1302:9; PTX-548. Mr. Muniz received a demonstration of Centripetal's patented RuleGATE product, which he described in an online blog that educates Cisco employees entitled "Cool Tool: Centripetal Networks RuleGate – Threat Intelligence Tool," and where he stated, "I found this tool to be a pretty cool new approach to leveraging threat data." Tr. 1299:16-1300:7; 1308:5-15; PTX-550 at 647-49, 51; *see also* PTX-549 at 645.

42. As further examples of Cisco's interest, in November and December 2016, Cisco had several meetings with Oppenheimer & Co., Inc. about Centripetal, pursuant to Centripetal's engagement with Oppenheimer to evaluate companies who were interested in making a strategic investment in Centripetal. Tr. 1234:17-25. In December 2016, Oppenheimer presented to Cisco additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGATE functionalities covered by the Asserted Patents. Tr.1235:11-1236:21, 1237:25-1238:19; 1242:11-1243:10; DTX-1270 at 1, 25, 27-28, 30.

43. From the time of Centripetal's and Cisco's first meeting in 2015 up until Cisco launched their new infringing products in June 2017, Cisco's engineers and employees visited Centripetal's website 354 times and viewed 1,206 webpages regarding its products. Tr. 1024:16-1025:4.

44. After all of these detailed meetings with Centripetal, Cisco released on June 20, 2017, its "network of the future" products that "stop[] security threats in their tracks," which incorporated Centripetal's patented technology. Tr. 1159:9-1161:5 (*citing* PTX-452 at 648); Tr. 900:21-901:14.

45. Centripetal's demonstrative, shown below and presented during opening statements, accurately reflects the evidence presented at trial surrounding the events of Centripetal and Cisco's relationship.



46. On November 8, 2017, after Cisco's Senior Director of Cybersecurity Investments and Acquisitions, Karthik Subramanian, expressed interest in receiving information about Centripetal and requested more technical information, which Mr. Rogers provided to him, including a "white paper explaining the intelligence led cloud service architecture for providers using our virtual enforcement points." Tr. 1245:8-1246:17; PTX-107.

D. Cisco Used Centripetal's Patented Security Technologies to Avoid Commoditization

47. Instead of becoming a distributor of Centripetal's technology, Cisco copied Centripetal's patented technology after having numerous meetings with Centripetal spanning several years in order to gather information about Centripetal's business, technology, products, and patents. Tr. 1214:13-20; 1295:6-21.

48. Cisco had been selling traditional network devices (switches, routers, and firewalls) for years before meeting with Centripetal. Cisco faced commoditization of these traditional network devices, and thus needed to differentiate itself in the market. Tr. 1451:12-

1458:5. In its 10-K filing with the SEC in 2016, Cisco described experiencing "increased competition . . . based on commoditized hardware." Tr. 1451:12-1452:21. Market analysts in 2016 noted the same thing, writing in an article that they "continue to see commoditization as a major challenge for Cisco's switching business." PTX-1460 at 993.

49. Cisco identified security as its needed market differentiator, writing in its 2016 10-K filing that security was "the top IT priority for many of our customers." Tr. 1451:12-1452:6; *see also* Tr. 1453:13-1454:24 (discussing PTX-560 at 771). Cisco further explained that "the most effective way to address security challenges is with continuous threat protection that is pervasive and integrated," *i.e.*, layers of security integrated into its routers, switches, and firewalls. Tr. 1451:12-1452:6; *see also* Tr. 1453:13-1454:24 (discussing PTX-560 at 771).

50. After learning about Centripetal's threat-intelligence-based security, Cisco released network infrastructure products with proactive embedded security features. Tr. 53:15-68:19; *see also* Tr. 1159:9-1162:14 (*citing* PTX-452 at 1); PTX-1135; Tr. 900:21-901:14. These products include switches, routers, firewalls, and systems that manage and support these products. Tr. 53:15-68:19.

51. Cisco thus addressed the problem of commoditization of its traditional networking products, at least in part, by implementing Centripetal's patented security technologies.

E. Cisco Announced its "Network of the Future" and Released the Accused Products Starting in 2017

52. Starting in 2017, Cisco launched its new router, switch, and firewall with "built-in" security to make and enforce rules protecting against network threats, nearly two years after its first meeting and within six months after its last meeting with Centripetal. *See, e.g.*, Tr. 733:3-735:3 (citing PTX-585 at 410).

53. In a press release dated June 20, 2017, Cisco touted its "network of the future" products that "stop[] security threats in their tracks," which incorporated Centripetal's patented technology. Tr. 1159:9-1161:5 (*citing* PTX-452 at 648); Tr. 900:21-901:14.

i. Catalyst 9000 Switch

54. After learning of Centripetal's threat-intelligence-based security, Cisco introduced a "new family of switches built from the ground up," termed the "Catalyst 9000 Switch," which was designed to "deliver[] unmatched security." Tr. 1160:8-1161:5 (*citing* PTX-452 at 649).

55. The accused "Catalyst 9000 Switch" includes the Catalyst 9300, 9400, 9500, and 9800 series running IOS-XE 16.5 and subsequent releases and the controller running IOS-XE 16.10 and subsequent releases. Tr. 434:14-17, 53:15-54:20; Dkt. No. 408 at 17.

56. The Catalyst 9000 Switch was launched in June 2017 and touted as "built for security" and "designed to enable customers to detect threats, for instance, in encrypted traffic" as part of "**a critical part of an end-to-end integrated security solution**, one that detects and stops threats." (emphasis in original) PTX-1260 at 849; PTX-1449 at 884.

57. Cisco's Catalyst 9000 Switches are embedded with infringing software code as part of a holistic security system. *See, e.g.*, Tr. 53:15-54:20; PTX-561 at 630; PTX-1303 at 56. In its 2019 10-K SEC filing Cisco described that, "Within campus switching are our Catalyst 9000 series of switches that include hardware with embedded software, along with a software subscription referred to as Cisco DNA." PTX-560 at 772.

58. Cisco released the Catalyst 9000 Switch to integrate proactive security capabilities within the network. Tr. 53:15-54:3. It can enforce a variety of security rules to

forward or drop packets. Tr. 39:15-40:4, 440:8-442:25, 450:23-452:11; *see also* PTX-1260 at 849.

ii. ISR/ASR Router

59. Cisco introduced the same security features in its new Catalyst 9000 Switch into its Integrated Services Router ("ISR") and Aggregation Services Router ("ASR") family of routers ("ISR/ASR Router") by updating its software on July 3, 2017, such as the ability to enforce network security rules that forward or drop packets. Tr. at 443:17-444:10; PTX-1195 at 1; PTX-1226.

60. The accused "ISR/ASR Router" includes the 1000 and 4000 series ISR and 1000 series ASR router running the operation system IOS XE 16.5 and subsequent versions. Tr. at 433:24-434:1, 54:21-55:12.

61. Cisco explained that its ISR/ASR Router now "include[s] integrated security, advanced analytics, automated provisioning, and application optimization, to deliver a complete solution." PTX-1226 at 638 (discussed in Tr. at 443:17-444:10). Cisco's ISR/ASR Router is also embedded with infringing software code. *See, e.g.*, PTX-561 at 630; PTX-1303 at 56; Tr. 54:21-55:12.

62. Cisco released the ISR/ASR Routers to provide performance, reliability, and integrate proactive security functionality within networks. Tr. 55:7-10.

iii. DNA Center

63. Cisco integrated its Digital Network Architecture ("DNA") technology into its Catalyst 9000 Switch and ISR/ASR Router, allowing its DNA Center to manage them with rules. Tr. 55:13-21, 575:15-577:8, 579:10-580:24; PTX-1294 at 3. DNA is an architecture that supports automation and "faster network services provisioning" and the ability to "[r]educe risk

with faster threat detection." PTX-1263 at 179. It configures and troubleshoots problems in the network. Tr. 55:13-21.

64. Cisco embeds DNA software in its Catalyst 9000 Switches and ISR/ASR Routers. *See, e.g.*, Tr. 1462:16-1464:16, 450:23-451:4, 578:25-580:5; PTX-1507 at 494-95; PTX-1248 at 265; PTX-1294 at 3.

65. DNA Center pre-processes rule sets, which Catalyst 9000 Switches and ISR/ASR Routers can swap without packet loss. Tr. 575:15-577:8, 579:18-580:24, 584:14-585:4, 586:15-587:18, 588:12-589:18, 597:10-601:8, 606:15-608:14, 633:24-634:14; *see also* 2571:12-2573:8; PTX-1294 at 3; PTX-1915; PTX-1195 at 1, 3-4.

66. DNA Center's primary function is to interact with and operate routers and switches providing the infringing capabilities. Tr. at 55:13-21, 450:23-451:24, 578:25-580:5, 593:12-594:11; PTX-1849 at 185. It is specifically designed to manage and send rules to the Catalyst 9000 Switches and ISR/ASR Routers, and thus it is integrated into the security solution that the switches and routers offer. Tr. 575:15-577:8; PTX-1263 at 179.

67. DNA Center may continually provision the Catalyst 9000 Switch and ISR/ASR Router so they are capable of being used effectively in the operation of the network. Tr. 56:1-7, 575:15-576:24. DNA Center uses advanced artificial intelligence and machine learning to observe past traffic on the network and has the capability to change configuration in the network in real time. Tr. 57:20-58:7. DNA Center takes that intelligence, operationalizes it, and processes rules and policies that the Catalyst 9000 Switches and ISR/ASR Routers use for security purposes. Tr. 451:3-24, 575:15-576:24.

68. Cisco touts DNA as a "feature" and "benefit" of upgrading to an infringing Router or Switch. *See, e.g.*, Tr. 1462:16-1464:16; PTX-1507 at 494; PTX-1248 at 265; PTX-1260 at 849.

iv. Stealthwatch

69. Cisco upgraded its Stealthwatch software ("Stealthwatch") to include, *inter alia*, a technology termed Cognitive Threat Analytics ("CTA") in 2017 to analyze traffic flowing through the Catalyst 9000 Switch and ISR/ASR Router to "detect and respond to threats in real-time." PTX-482 at 664; PTX-577 at 007; PTX-992 at 1-2; PTX-561; PTX-577; PTX-989; Tr. at 2342:4-7, 2148:8-25 (explaining the differences in release numbers for Stealthwatch, noting that CTA was added to Stealthwatch in 2017). CTA has various features for monitoring the network. For example, CTA monitors for security breaches within the network by using machine learning. Tr. 60:7-23. CTA is embedded in Stealthwatch. *See, e.g.*, Tr. 60:21-23.

70. Stealthwatch's analysis involves correlating traffic that enters and leaves devices in the network to determine whether the traffic contains a threat. Tr. at 59:1-7; 994:18-995:21; PTX-1065 at 5. Detected malicious traffic can be "blocked or quarantined by Stealthwatch," which involves sending rules to the Catalyst 9000 Switches and ISR/ASR Routers. PTX-584 at 403.

71. Stealthwatch is part of Cisco's Digital Network Architecture and is specifically designed to be used as an integrated system with Cisco's Catalyst 9000 Switches and ISR/ASR Routers. Tr. 450:23-452:11, 453:16-454:20. Cisco describes in a 2018 data sheet that DNA Center's "[i]ntegration with Cisco Stealthwatch© security provides detection and mitigation of threats." PTX-1281 at 1.

72. Cisco touts Stealthwatch as a "feature" of its Catalyst 9000 Switch and ISR/ASR Router and sells them "as one product." *See, e.g.*, Tr. at 1462:16-1464:16; PTX-1507 at 495; PTX-1260 at 849.

73. Stealthwatch was also upgraded around mid-2017, adding a technology called Encrypted Traffic Analytics ("ETA") in addition to adding the functionality of CTA. Tr. 59:10-15; PTX-452 at 648; PTX-1065 at 1.

v. Identity Services Engine

74. Cisco's Identity Services Engine ("ISE") software provides "[c]entral network device management" and "granular control of who can access which network device." PTX-411 at 891. ISE ensures user control over the network from any location. Tr. 61:8-16. It also provides network-based security regardless of location of the user. Tr. 61:8-16. ISE is responsible for tracking the identity of users and user computers on a network and for setting the limits of user and computer access to other devices in the network. Tr. 149:20-23.

75. Stealthwatch and ISE "work together" as "an integrated solution." Tr. 1466:18-1467:11; PTX-1035 at 1-2; PTX-1896 at 5; PTX-965 at 2803. ISE can be used with the Catalyst 9000 Switch and ISR/ASR Router to help protect networks from threats, even in encrypted traffic. Tr. 730:11-731:24, 732:14-21, 909:24-912:12, 958:9-25, 1119:10-1120:7; PTX-1284 at 2; PTX-989 at 33; PTX-563 at 415.

76. ISE is specifically designed to be used as an integrated system with Cisco's Catalyst 9000 Switches and ISR/ASR Routers, as well as with Stealthwatch. Tr. 1002:11-1003:1; PTX-1089 at 238 (showing how Netflow goes from the accused switches and router to Stealthwatch, Stealthwatch issues commands to ISE, and ISE issues rules to the accused routers and switches).

vi. Firewall

77. Cisco designed a new architecture for its Adaptive Security Appliance ("ASA") firewalls with Firepower and its Firepower Appliance Firewalls around late 2017 by adding Threat Intelligence Director ("TID") to the Firepower Management Center ("FMC"). Tr. 555:11-558:20; PTX-1883; PTX-1289 at 1, 1593.

78. Centripetal collectively refers to the following accused products as "Firewalls." The accused ASA firewalls include Cisco's Adaptive Security Appliance 5500 with Firepower services (version 9.4 and later). The accused Firepower firewalls include Cisco's Firepower Appliance 1000, 2100, 4100, and 9300 series that run Firepower Threat Defense 6.0 and later.

79. Cisco newly equipped its Firewalls in late 2017 to operate proactively with packet filtering functionality, particularly in connection with the TID. PTX-1291 at 7; Tr. 648:21-649:5, 651:18-653:6. Tr. 151:23-25.

80. Cisco's Firewalls provide a new level of network security based on threat indicators with new rules that can be swapped efficiently in the devices. Tr. 648:21-649:5, 651:18-653:6, 655:10-656:20, 673:6-675:5, 679:18-681:10, 694:22-696:12, 698:8-22; PTX-1293 at 668; PTX-1196 at 7.

81. The infringing software code is embedded into the Firewalls. Tr. 662:15-663:9; PTX-1849 at 91, 93.

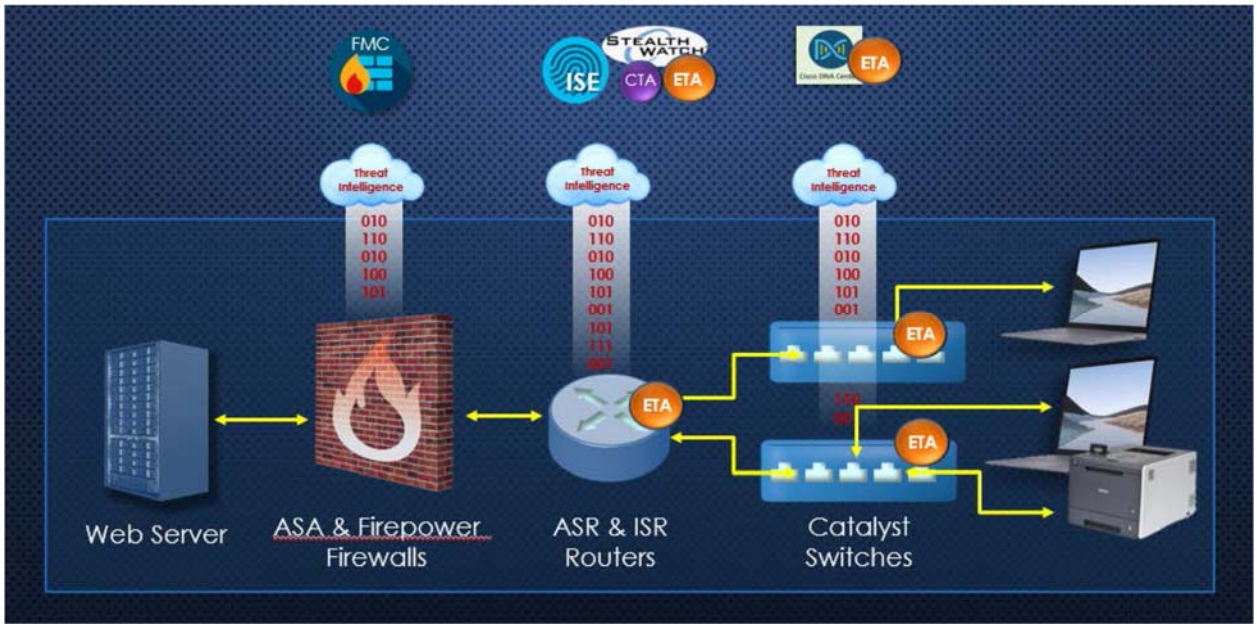
vii. Firepower Management Center

82. Cisco designed a new management software for its Firewalls integrating them with FMC version 6.0 and later. The FMC also includes TID, which receives rules from various sources and preprocesses them into a rule set. Tr. 558:1-20; PTX-1289 at 1593; PTX-1196 at 7.

83. FMC operates the Firewalls and provide functions such as managing the network at that particular point in the network, protecting against malware, and checking and proactively blocking attempts at malicious intrusions into the network. Tr. 63:24-64:10. FMC can configure and operate multiple firewall devices in the network. Tr. 643:6-10; Tr. 558:1-14.

viii. Summary of Accused Products

84. Centripetal's final tutorial slide depicts a Cisco network that utilizes all of the Accused Products as intended to protect network (Tr. 67:6-68:19):



85. A table of Centripetal's Patents along with Cisco's infringing products (collectively, "Accused Products") is below:

Centripetal's Patent	Accused Cisco Products
'193 Patent	Catalyst 9000 Switch
	ISR/ASR Router
'806 Patent	Catalyst 9000 Switch with DNA Center
	ISR/ASR Router with DNA Center
	Firepower/Adaptive Security Appliance Firewall with Firepower Management Center
'176 Patent	Catalyst 9000 Switch with Stealthwatch
	ISR/ASR Router with Stealthwatch

III. FACTS RELATED TO CENTRIPETAL PRACTICING ITS ASSERTED PATENTS

86. Centripetal's RuleGATE product practices the patents in this case. Tr. 1381:13-1383:12, 1384:12-1385:19; PTX-1215.

87. Cisco did not dispute that RuleGATE practiced the Asserted Patents.

88. PTX-1215 describes how RuleGATE practices the Asserted Patents. Tr. 1384:8-1385:19; PTX-1216 at PDF pages 26-44 ('193 Patent), 45-69 ('806 Patent), 85-106 ('176 Patent).

89. The technology in Centripetal's RuleGATE product that practices the '193 Patent is its capacity to prevent data transfers from one network to another, which it does using a hardware processor and memory. Tr. 1384:12-20.

90. The technology in Centripetal's RuleGATE product that practices the '806 Patent is its ability to handle cyber threat intelligence using dynamic sources that allow the RuleGATE to use a myriad of threat indicators, which it can seamlessly switch for updating without dropping packets. Tr. 1384:21-1385:6.

91. The technology in Centripetal's RuleGATE product that practices the '176 Patent is its capacity to correlate different network flows and identify which flows are associated with a particular host that may be compromised. Tr. 1385:7-15.

IV. FACTS ON THE OVERVIEW OF THE TECHNOLOGY

A. Overview of Networking

92. The three principal devices that comprise computer networks are switches, routers and firewalls. Tr. 19:21-20:10.

93. Beginning with switches, Centripetal's expert Dr. Medvidovic used analogies to explain these complex network devices and compared the operation of a switch to that of a

telephone switchboard operator. Tr. 20:13-22. Therefore, similar to an operator connecting people, switches in a network operate to automatically connect different devices together such as a computer with another computer or a computer to a printer. Tr. 20:24-21:2; *see* Fig. 1.

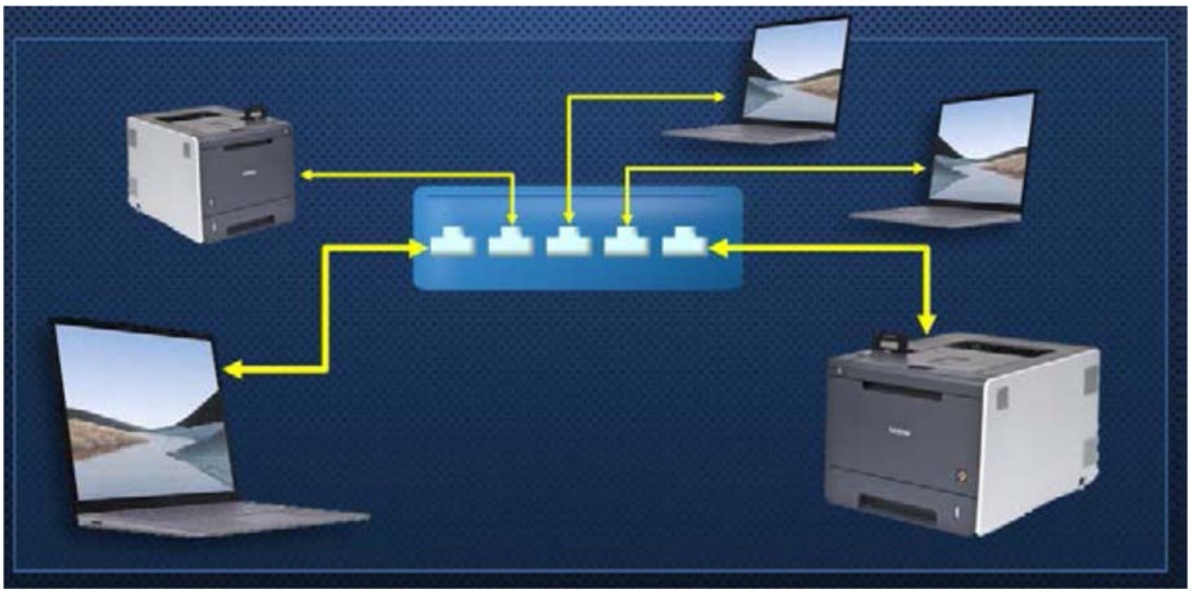


Fig. 1.

94. Comparatively, routers function similarly to a 911 dispatcher who sends and controls the distribution of emergency vehicles to the intended location. Tr. 22:9-19. Routers decide the most optimal way to automatically send computing data to a desired location. Tr. 22:24-23:2. They are constantly evaluating current computer traffic and sending data along the most efficient path to its intended destination. Tr. 23:8-14. The combination of routers and switches are the fundamental building blocks of computer networks. Tr. 23:17-23. Together, switches connect local devices into small networks and routers operate to transmit data between these smaller networks – thus forming larger networks. Tr. 23:17-24:3; see Fig 2.

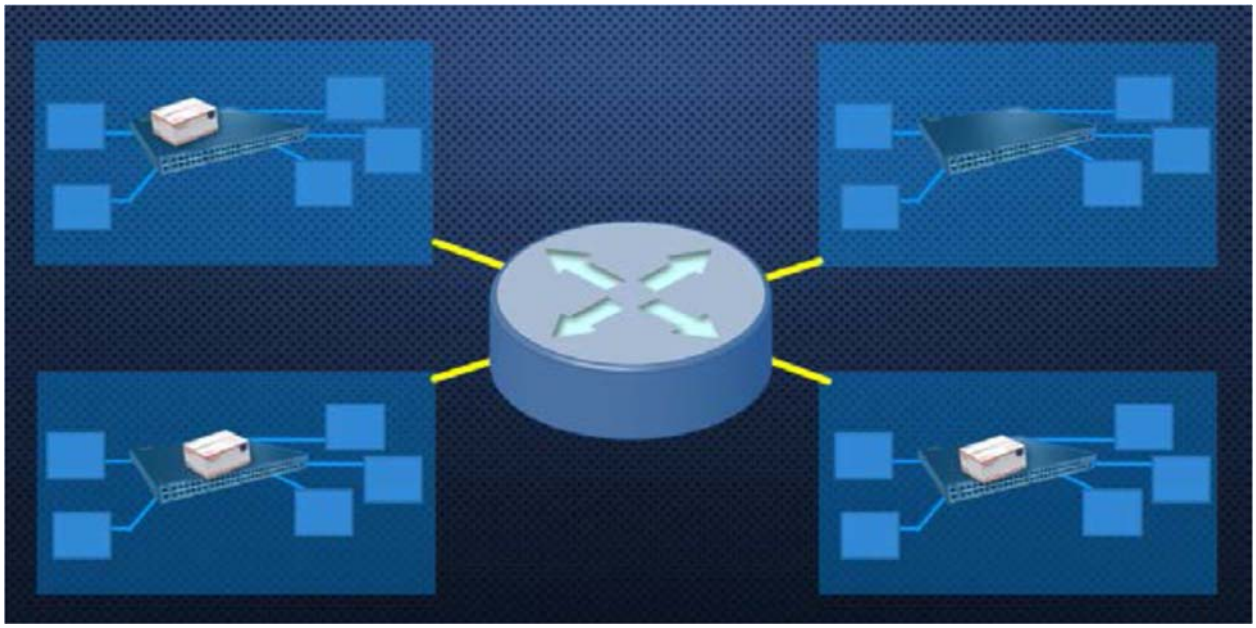


Fig. 2.

95. Firewalls, in the context of computer networking, are similar to that of a firewall in an office building or hotel. Tr. 24:13-19. They operate to automatically put a "wall" between valuable assets and any potential danger. *Id.* Therefore, data entering a network is often transmitted in through a firewall and the firewall can perform a variety of functions, such as disallowing the data to enter the network by blocking it. Tr. 24:23-25:4; see Fig. 3.

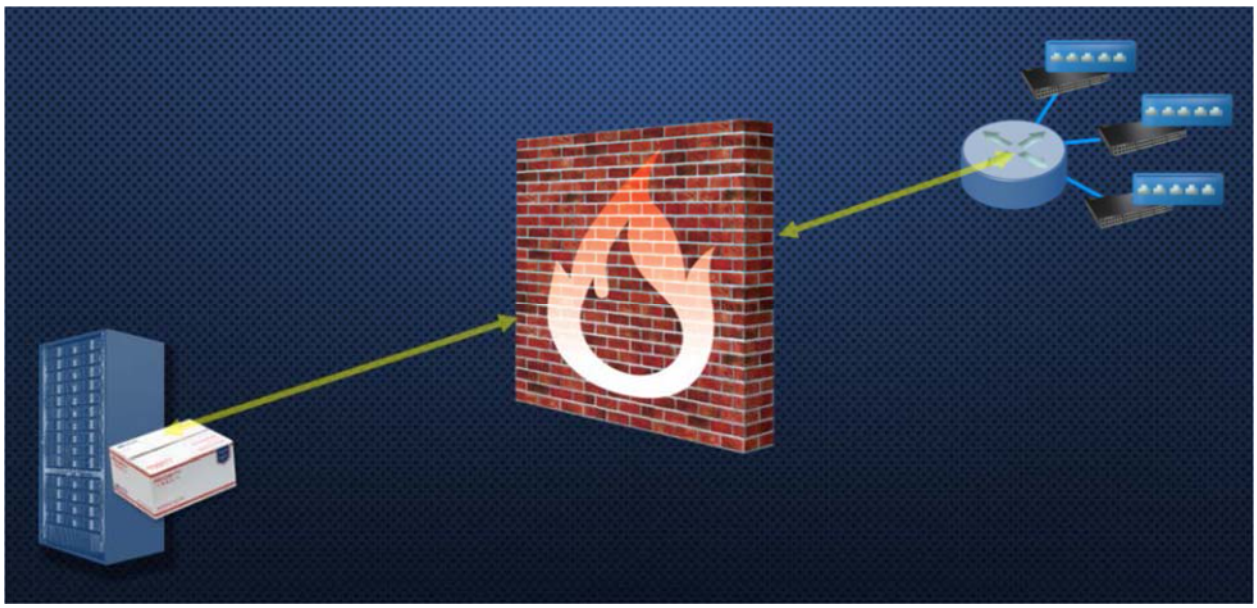


Fig. 3

96. Dr. Medvidovic used video access to ESPN.com from a web server as an example of the operation of a firewall. He explained that:

> [A]ny data you try to see or retrieve from the ESPN servers would be on that web server. And that data would travel to you, but before it gets to your computer, it would first go through this firewall, and the firewall may decide to permit that data to go through because it does not violate any policies or rules that you may have for the firewall. . . . So for example, it [the firewall] could be in a company where the company policy is you can't watch sports during work hours. So in that case, that data from ESPN would be dropped at the firewall and never arrive to you.

Tr. 25:8-20. Accordingly, firewalls often sit at the edge of individual networks to control the entry of data from the internet. Tr. 26:2-12. As technology develops, firewall-type functionality is often now included inside of other devices such as routers and switches. These devices may be located at different locations within a network – not just at the outside barrier. Tr. 82:8-18. This inclusion of firewall functionality in other devices is in contrast with older network technology where firewalls were responsible for the security of the network, by blocking malicious packets from entering it, while the routers and switches focused on speed and performance in the transmitting data. Tr. 26:16-22.

97. The combination of thousands of these networking devices into larger and larger networks is responsible for the creation of nationwide networks and the global internet. Tr. 23:24-24:3. Therefore, the global internet as we know it is a network of networks. Tr. 74:1-12. Internet providers, such as Earthlink, Verizon, AT&T, and Cox are in the business of creating large scale networks to connect users to other business networks in order to access data. Tr. 74:1-12, 76:10-19. Companies like Netflix, Facebook, Zoom, Google and Amazon operate their own independent networks that connect to the larger internet to send data across the internet to end-users. Tr. 75:23-76:9; *see* Fig. 4.

Fig. 4

98. The international nature of the internet requires that the sending of data between all of these providers be based on uniformly developed standards that are globally applicable. Tr. 77:5-17. One such organization, the Internet Engineering Task Force ("IETF") is responsible for developing universal internet related standards. *Id*.

99. There are many different standards that are developed to facilitate the transmission of data over the internet. *Id*. These standards are often in the form of protocols, which are the rules of engagement for two computers that specify how the two computers can work together to communicate back and forth. Tr. 954:5-17.

100. For example, the Hypertext Transfer Protocol ("HTTP") is used in web pages to transfer data over the internet from computer to computer, the Internet Protocol ("IP") is a building block in allowing data to use interconnected networks, and the Transmission Control Protocol ("TCP") is used to deliver information across the internet. Tr. 77:23-78:2, 89:18-21. These protocols are the methods used by nationwide and global networks. Tr. 88:19-21.

101. The transmission of computing data through these devices is done in the form of a network packet or packets. Tr. 26:23-28:14. The packet is similar to that of a package sent through the United States Postal Service. Tr. 26:23-28:14, 89:2-3.

102. For example, when a user on their computer attempts to watch a video from ESPN.com, that video is a very large amount of information and cannot efficiently be sent in one package and is therefore, broken up into a number of smaller units known as packets. Tr. 27:3-14. The packet will flow from the internet and through multiple devices on the network and transmit the requested information to the end user. Tr. 88:1-14. At any time, there are trillions of packets being exchanged through global networks. Tr. 88:16-19. Packets consist of two different parts: the header and the payload, as shown below in Fig. 5.

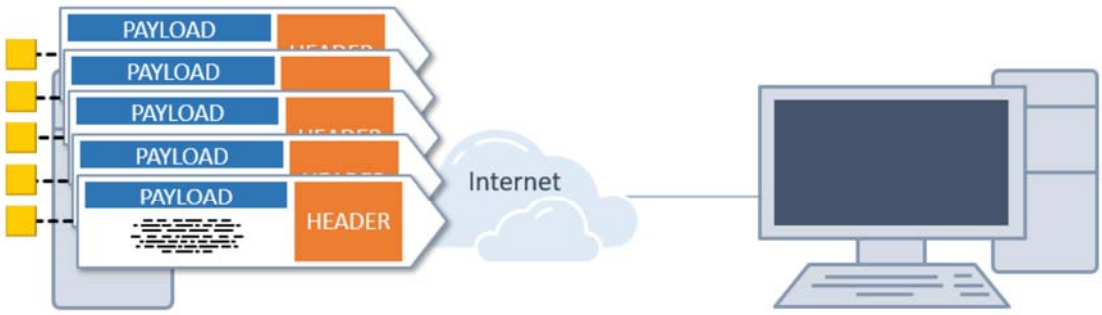


Fig. 5

103. The header contains information such as the source address, source port, destination address, destination port number, and the protocol being used to transmit the packets. Tr. 107:16-23. These five pieces of information are known as the "5-tuple." Tr. 108:2-4.

104. The information contained in the header is inspected by the router or switch to determine where and how to send that individual packet. Tr. 108:7-16. This information can be

thought of as a mailing label on a package which contains an individual's name and mailing address as well as a return address. Tr. 27:24-28:1.

105. The payload is the portion of the packet that contains the actual content of the data, and in the ESPN video hypothetical, this would be the actual portion of the video sent by each individual packet. Tr. 28:4-10. This data in the payload part of the packet can be encrypted, meaning the information in the payload can be transmitted in code. Tr. 28:18-25.

106. For example, the hypothetical video from ESPN.com would not usually be encrypted, but often data sent in a packet's payload containing sensitive information, such as banking or credit card data, will be encrypted. Encryption becomes vital so that this sensitive data is not stolen by bad actors hacking the network. Tr. 28:18-25. Encryption works to lock up the data in the payload section of the packet so it cannot be seen without decryption. Tr. 28:25-29:5. Consequently, just as with a sealed package, snoopers of network traffic would be unable to see what is in the packet unless it could be unlocked and opened, which is generally known as decrypting the data. But, even when a packet is encrypted, the header information, such as the source and destination, is not encrypted and is visible. Tr. 29:10-16; see Fig. 6.

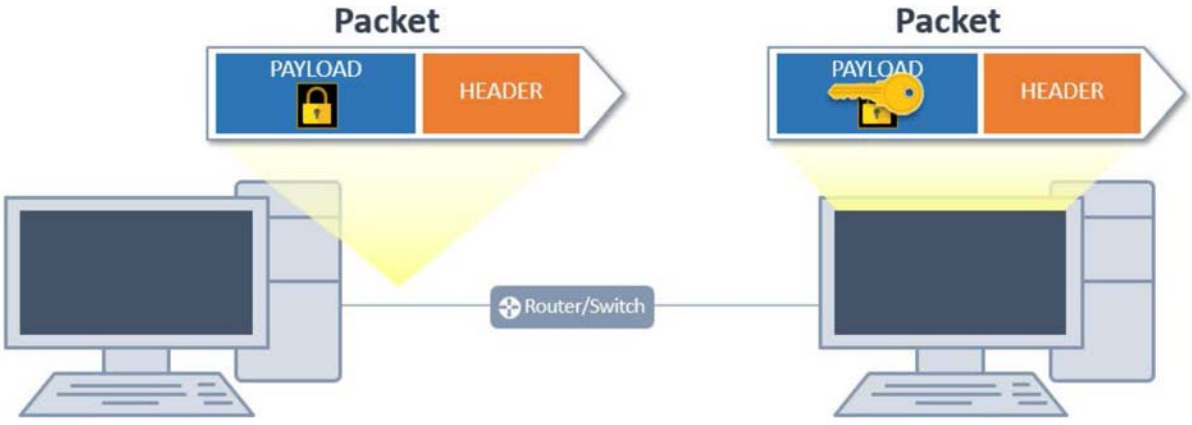


Fig. 6

107. As previously noted, the hypothetical ESPN video is set in a collection of packets that comprise the video. The collection of all the packets together that make up the transmitted video is known as a packet flow. Tr. 106:15-16. Thus, the header of each packet in this particular flow would contain identifying information that distinguishes this collection of packets from other flows. Tr. 107:16-23. This allows for routers to keep the packets in order and properly distribute the packets to the correct destination.

B. Overview of Networking Security

108. The internet is a very large and complex organization of networks that utilize protocols to relay data from one network device to another resulting in the transmission of data to an end user. Tr. 112:1-6. As a result of the internet's complexity, there are many methods employed by cyber criminals to transmit malware and gain access to encrypted, secure and confidential information. Tr. 112:7-14. Cyber criminals can use malware or other methods to infect a network and steal data using a process known as exfiltration. Tr. 343:19-15. Exfiltration is the process by which cyber criminals "exfiltrate" data out of a network by stealing valuable confidential data. Tr. 343:19-25.

109. To prevent malware and data exfiltration, cyber defense systems often use a concept known as defense-in-depth, the deployment of a variety of network security devices at different layers of the network, to protect sensitive network data. Tr. 140:1-12, 144-5-11.

110. Cisco's expert, Dr. Almeroth, compared network defense-in-depth to that of the security used by a federal courthouse, which contains a series of secured entry points to the building, a courtroom or a judge's chambers. Tr. 112:18-22. Consequently, just like any type of modern security system, there must be different layers of security in a network to be effective in preventing evolving methods of cyberattacks. Tr. 113:3-10, 51:17-21. Therefore, to maximize effectiveness, security measures are often placed at different devices/locations in a network, such

as within a firewall, a security gateway, in routers and switches, and also within the end user's computer. Tr. 113:11-18.

111. Some security technology focused on a firewall at the border of the network to detect and block malicious packets from entering a network. Tr. 118:8-119:25. The process begins when a packet is sent from the internet to another smaller network. A firewall device, usually located at the entry of the network, operates by inspecting information in the packet to determine if that packet is malicious. Tr. 119:18-25. This process is completed by matching information from the header or payload of the packet to rules that are pre-enabled in the firewall type device. Tr. 119:18-25. These rules are comprised of previously known information about sources of malicious or otherwise unauthorized traffic. Tr. 122:11. Thus, if information from a packet header is matched to a rule, then the packet is unauthorized to enter the network and is blocked / dropped. Tr. 120:6-12.

112. A blocked packet is thrown away. Tr. 120:15-18. If there is no rule that matches the packet, the packet is allowed to proceed into the network and to its final destination. Tr. 120:2-5.

113. Rules are the mechanism that determines which packets are allowed in and out of the network. The collection of rules that are being applied by network devices can also be referred to as Access Control Lists ("ACLs"). Tr. 537:18-21, 2550:1-4. Threats are continually evolving, and as a result, rules can be automatically updated or swapped in switches, routers and firewalls by other management devices in the network that intake "threat intelligence" information. Tr. 126:5-11. Threat intelligence information is an everchanging collection of information from known viruses and malware that is compiled by third-party providers. Tr. 126:5-11. Devices that manage switches, routers and firewalls often operate by digesting threat

intelligence, converting that intelligence into rules, and sending those rules out to intra-network devices such as firewalls, routers and switches that match rules to packets. Tr. 126:5-11. The ability to apply measures in real-time to new or different rules after the packet has cleared the gatekeeping firewall is called proactive security, which is a newer and more effective technology. Tr. 321:1-323:10.

114. This process of proactively blocking packets as they travel through the network comes with distinct challenges. The efficacy of this method rests on the ability of network devices to continually apply new or different rules to packets. Therefore, as the volume of packets and rules increase, so must the number of devices or the processing speed of current devices to remain effective. Tr. 124:6-19. Without increased speed or adding hardware, there will be extensive delay/latency because the system will be overwhelmed trying to match new or different rules to an overwhelming number of packets. Consequently, this delay can affect user performance on the network (i.e., increase web page loading times). Tr. 126:20-24. Another issue is that a network might have different entry points or destination points for data. Tr. 127:5-8. Therefore, firewall capable devices must be placed at all possible entry and destination points or risk that data could reach an improper destination without the application of updated rules. Tr. 127:5-8.

V. FACTS RELATED TO INFRINGEMENT AND VALIDITY OF THE '193 PATENT

115. The '193 Patent was referred to as the "Forward or Drop / Exfiltration Patent" at trial. Tr. 2356:2-6.

116. The '193 Patent was filed on February 18, 2015 as a continuation of Application No. 13/795,822, giving the '193 Patent a priority date of March 12, 2013. JTX-4.

117. The '193 Patent issued June 20, 2017. JTX-4.

118. The priority date of the '193 Patent is March 12, 2013. JTX-4.

119. The '193 Patent expires on March 12, 2033. JTX-4.

120. The asserted claims of the '193 Patent are Claims 18 and 19. Dkt. No. 411 at 2. Claims 18 and 19 are, respectively, a packet filtering system and computer readable media claim.

121. Computer readable media is software comprising of source code that is loaded into computer hardware through a device such as a CD-ROM, memory card or flash drive. This media comprises of readable instructions for the intended computer to operate. Tr. 473:3-23.

122. Claim 18 is laid out below:

> A system comprising:
>
> at least one processor; and
>
> a memory storing instructions that when executed by the at least one processor cause the system to:
>
> > receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;
> >
> > responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:
> >
> > > apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and drop each packet in the first portion of packets; and
> >
> > responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:
> >
> > > apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and forward each packet in the second portion of packets toward the third network.

JTX-4.

123. Claim 19 is identical to Claim 18 in every respect except it is a computer readable media claim. JTX-4. Claim 19 substitutes the introductory language of Claim 18, "A system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to . . .", with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to: . . . ." JTX-4; *see* Tr. 472:21. For purposes of infringement, the parties addressed the preambles of Claims 18 and 19 separately and the remainder of the claim limitations at the same time.

124. Dr. Sean Moore, one of the inventors of the '193 Patent, testified that the technology claimed in the patent centered around preventing the exfiltration of confidential data by cyber criminals. Tr. 343:12-16.

125. Centripetal's expert, Dr. Mitzenmacher, testified that the Asserted Claims of the '193 Patent are related to the process of forwarding and dropping packets for the purpose of preventing exfiltrations. Tr. 465:16-21. Additionally, Dr. Mitzenmacher opined that the '193 Patent applies to the prevention of many different types of data exfiltration. Tr. 467:10-468:17.

126. Exfiltration can occur in the context of cyber criminals hacking into the network and stealing data, but it also can occur within networks internally. For example, within one large corporate network there are many different departments or subnetworks, such as finance and human resources. *See* Tr. 490:17-25. It is common within these multi-departmental companies that certain departments have access to confidential materials, while for others that access is restricted. Tr. 467:10-468:7.

127. Accordingly, the network must restrict the ability of packets with this sensitive information to travel to unauthorized internal departments and external networks, while also

allowing packets with no sensitive information to be freely transmitted to other employees within the network. Tr. 467:14-468:17.

128. The '193 Patent specifically identifies a process by which rules can be enabled to filter packets of data depending on the type of data transfer that is being transmitted throughout the network. Tr. 468:18-469:9.

A. Infringement of the '193 Patent

i. Overview of Infringement

129. Centripetal accuses Cisco's Catalyst 9000 Switch and ISR/ASR Router of infringing Claims 18 and 19 of the '193 Patent. Tr. 433:12-434:1. The Catalyst 9000 Switch and ISR/ASR Router perform all elements of the accused functionality. Tr. 804:11-23.

130. The Catalyst 9000 Switch and ISR/ASR Router share the same operating system known as IOS XE. Tr. 448:11-24, 449:19-450:4; PTX-242 at 816-17.

131. Cisco compiles the source code that operates the Catalyst 9000 Switch and ISR/ASR Router in the United States. Tr. 462:4-463:18, 464:4-14; PTX-1409 at 5-6.

132. Cisco uses its own switch and router products, including Cisco's Catalyst 9000 Switch and ISR/ASR Router in its own networks. Tr. 1668:20-1671:10.

133. The Catalyst 9000 Switch and ISR/ASR Router contain processors and memory that stores software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 056. One of the processers within the Accused Products are programmable Applied Specific Interred Circuits ("ASIC"), known as Unified Access Data Planes ("UADP"). Tr. 477:23-478:8; PTX-1262 at 994. This type of processer is commonly referred to as a UADP ASIC. Tr. 477:23-478:8; PTX-1262 at 994; PTX-1390 at 29.

134. In their operation, the processors work within the Catalyst 9000 Switch and ISR/ASR Router to receive and transmit packets across a network. PTX-1276 at 216; Tr. 488:1-

489:3. During the transmission of packets, the operating system (IOS XE), working in conjunction with UADP ASICs, apply a variety of different rules to packets to determine if the packet should be permitted or dropped. PTX-1276 at 216.

135. The technical documentation for the Catalyst 9000 Switch and ISR/ASR Router operating system shows that the switches and routers support the application of multiple different ACL rule sets including: Port ACL ("PACL"); Vlan ACL ("VACL"); Router ACL ("RACL"); Client Group ACL ("CGACL"); Security Group ACL or Role Based ACL ("SGACL" or "RBACL"). PTX-1276 at 216.

136. ACLs are often applied to packets on ingress into the device and egress out of the device. PTX-1276 at 216. To simplify the process of applying rules, Cisco's IOS XE utilizes a specific method where labels are applied to packets. These labels are known as Secure Group Tag / Scalable Group Tag ("SGT"). Tr. 494:12-24; *see* PTX-1276 at 211. Cisco's non-infringement expert, Dr. Crovella, confirmed that Secure Group Tag and Scalable Group Tag are in fact the same. Different names are being used at different times because of a marketing change. Tr. 2420:1-17.

137. SGTs are attached to categorize network traffic. PTX-1280 at 21. SGTs can also be based on a variety of information, including the 5-tuple, type of traffic and application. Tr. 2400:11-25 (Dr. Crovella, Cisco's expert witness, highlighting that a quarantine rule has the ability to look at all information in the 5-tuple).

138. As packets enter the Catalyst 9000 Switch and ISR/ASR Router, they perform an initial check to see if there is a specific SGT attached to each packet that is entering through the switch or router. Tr. 2420:20-2421:8.

139. After the initial check, the Catalyst 9000 Switch and ISR/ASR Router applies an initial collection of rules known as a Group Access Control List ("GACL"). SGACL is also applied that blocks or permits packets specifically based on SGTs. Tr. 2389:1-3; PTX-1276 at 216; *see* Tr. 2423:5-2424:15.

140. On a packet's ingress into the device, the Catalyst 9000 Switch and ISR/ASR Router applies an input SGACL based upon the SGT. Tr. 2389:1-8; *see* PTX-1288 at 12 (showing input GACL applied based on ingress client); *see also* PTX-1276 at 216; PTX-1390 at 86 (2019 document).

141. On a packet's egress out of a device, the Catalyst 9000 Switch and ISR/ASR Router applies an output SGACL based upon the SGT. Tr. 2389:15-19; *see* PTX-1288 at 12 (showing output GACL applied based on egress client); *see also* PTX-1276 at 216; PTX-1390 at 86.

142. Cisco's expert, Dr. Crovella, confirms that SGACLs are applied on a packet ingress into the Catalyst 9000 Switch and ISR/ASR Router and applied on a packet's egress out of the switch or router. Tr. 2389:15-19, 2399:20-22; PTX-1288 at 12.

143. The SGACL rule-based packet blocking by comparing SGTs is commonly referred to by Cisco as rapid threat containment, segmentation, or quarantining. Tr. 2383:11-19, 2423:9-15.

144. The quarantine rule operates to block particular types of data transfers between certain networks while allowing others. Tr. 493:24-495:14, 496:14-497:13, 536:23-537:1, 2419:3-15; *see* PTX-1262 at 999.

145. The Catalyst 9000 Switch and ISR/ASR Router determines whether the packet should be permitted or blocked based on the SGT. Tr. 535:10-17; PTX-1280 at 21; *see* PTX-

1262 at 999. This process is completed by the Catalyst 9000 Switch and ISR/ASR Router by applying operators, such as permit or deny, to incoming and exiting packets based upon their assigned SGT. Tr. 531:16-21; PTX-1280 at 21.

146. If a packet's SGT is not correlated to a SGACL rule on either ingress or egress, then a permit operator is applied to the packet, and it is permitted to be transmitted through the router or switch to its intended network. Tr. 542:17-24; PTX-1288 at 12. But if an SGT matches one of the SGACL rules because the data transfer is not permitted, a deny operator is applied, and subsequently the packet will be blocked. Tr. 545:8-546:12, 548:11-19; PTX-1288 at 12.

147. Contrary to Cisco's position, the Asserted Claims do not require inspection of the payload of a packet. Instead, the Asserted Claims require the enforcement of a packet filtering rule that inspects a packet and applies an operator. Tr. 3048:11-3049:1 (apply packet filtering rule and then you apply the operator).

148. Cisco directed its customers to use the Catalyst 9000 Switch and ISR/ASR Router as they were described in Cisco's documents, including marketing material, manuals, and source code.

149. Cisco was at least aware of the '193 Patent and the manner its customers infringed the '193 Patent when Centripetal filed the complaint in this case naming the '193 Patent, the Accused Products, and described the manner in which the Accused Products were used to infringe.

ii. Element-by-Element Analysis

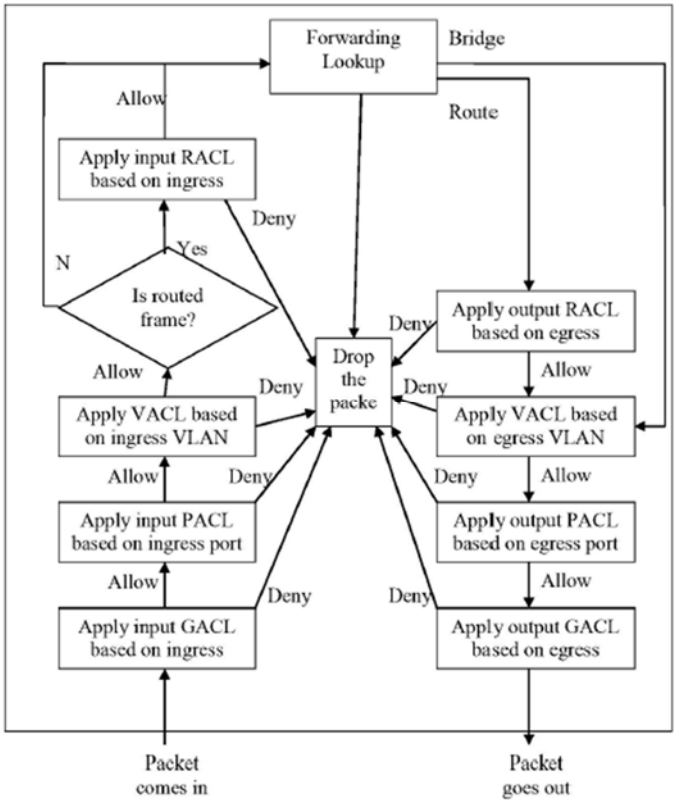
(a) ***A system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:***

150. The Catalyst 9000 Switch and ISR/ASR Router all have processors and memory. The memory stores instructions that are executed by the processor to cause the operation of the system. Tr. 473:3-485:13; PTX-1303 at 56; PTX-175 at 598-99; PTX-1313 at 18.

(b) ***receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;***

151. The Catalyst 9000 Switch and ISR/ASR Router receive packets from other devices both inside and outside the network. Tr. 485:14-489:9; PTX-1276 at 216.

152. PTX-1276 at 216 is a document created by Cisco that shows its products receive incoming packets:



PTX-1276 at 216.

(c) ***responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:***

153. The Catalyst 9000 Switch and ISR/ASR Router have rules to block packets being transferred between networks if certain types of data transfers are detected. Tr. 489:17-502:10, 504:14-514:10, 516:8-521:4; PTX-576 at 991; PTX-1262 at 999; PTX-1280 at 21; PTX-563 at 414-15; PTX-1849 at 9, 21, 228; PTX-1911.

154. The Catalyst 9000 Switch and ISR/ASR Router can block data exfiltration attempts using a quarantine rule. Tr. 492:7-493:9; PTX-576 at 991.

155. The Catalyst 9000 Switch and ISR/ASR Router implement quarantine rules to block packets using policies in their Access Control List (ACL) that are applied to certain Scalable Group Tags (SGTs). Tr. 493:22-502:10, 518:22-520:13; PTX-1262 at 999; PTX-1280 at 21; PTX-563 at 414-15.

156. When a device or group of devices are quarantined, SGTs are added which detail the networks and types of data transfers that are allowed or not. Tr. 505:14-506:14; PTX-1849 at 9 (shows code showing that the Catalyst 9000 switch and ISR/ASR Router are capable of using SGT tag for quarantine) and 21 (showing code for the ACL applying the SGT).

157. The Catalyst 9000 Switch and ISR/ASR Router implement "rapid threat containment" when they cause packets associated with a quarantine rule to be blocked from some networks and not blocked for other networks. Tr. 500:10-502:10, 506:19-509:4; PTX-563 at 414-15; PTX-1849 at 21; PTX-1280 at 21.

158. The excerpt from PTX-1280 at 21, shows that a quarantine rule is applied from the SGT and will limit an endpoint's network access by blocking packets:

Notice above that rapid threat containment is seamless in SD-Access fabric, as the endpoint continues to be operational in the employee VLAN and the IP address remains unchanged. However, the SGT assignment has changed from 4 to 255, which is the quarantine SGT.

Fabric edge devices will then download SGACL permissions specific to SGT 255, which will limit the endpoint's network access until a successful remediation is performed.

PTX-1280 at 21.

159. The excerpt from PTX-576 at 991, shows that the Catalyst 9000 Switch and ISR/ASR Router are designed to use rules to block exfiltration traffic:

Engine	What It Does
Data exfiltration	Analyzing more than 10 billion web requests per day, Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. CTA recognizes data exfiltration even in HTTPS encoded traffic, without any need to decrypt transferred content.

PTX-576 at 991.

160. The Catalyst 9000 Switch and ISR/ASR Router are designed to implement quarantine rules based on detecting abnormal behavior in a variety of data transfer types, including Hypertext Transfer Protocol (HTTP), HTTP GET, and HTTP POST. Tr. 510:18-513:2, 516:8-518:7, 520:15-521:2; PTX-1849 at 228; PTX-1911.

(d) ***apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and***

161. The Catalyst 9000 Switch and ISR/ASR Router will apply an operator corresponding to a quarantine rule to drop certain packets based on their association with certain types of data transfers. Tr. 521:8-536:19; PTX-1356 at 1; PTX-1326 at 11; PTX-563 at 415; PTX-1280 at 21; PTX-1912.

162. The "rapid threat containment" will apply a deny operator from a quarantine or other rule to cause the packets to be dropped if they are identified as engaging in dangerous types of data transfer. Tr. 524:1-526:7, 531:5-21; PTX-1356 at 1; PTX-1280 at 21; PTX-1912.

163. The excerpt from PTX-1356 at 1 shows how rapid threat containment will use rules to quarantine endpoints that are identified as infected with malware:

Rapid Threat Containment in SD-Access

Introduction

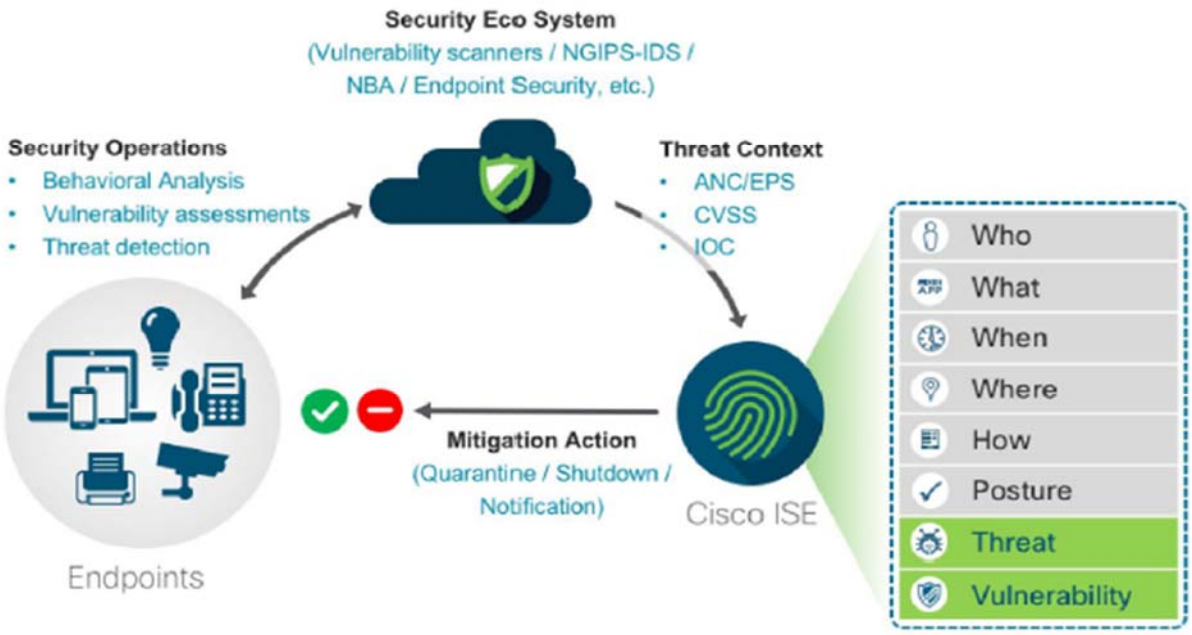
Rapid Threat Containment (RTC) is the process by which an endpoint can either be isolated or quarantined after having been identified as infected by malware or having been in violation of an established policy in the network. The actual detection may be the result of a violation of a traffic or group policy defined within Stealthwatch and determined through exported NetFlow records, next generation firewall application inspection, or AMP for endpoints detection.

PTX-1356 at 1.

164. The Catalyst 9000 Switch and ISR/ASR Router are designed to be able to change their status. Tr. 526:9-527:17; PTX-1326 at 11.

165. The excerpt from PTX-1326 at 11, shows how the Catalyst 9000 Switch and ISR/ASR Router are designed to change their status to block exfiltration traffic:

1.6.2 How does Rapid Threat Containment work



PTX-1326 at 11.

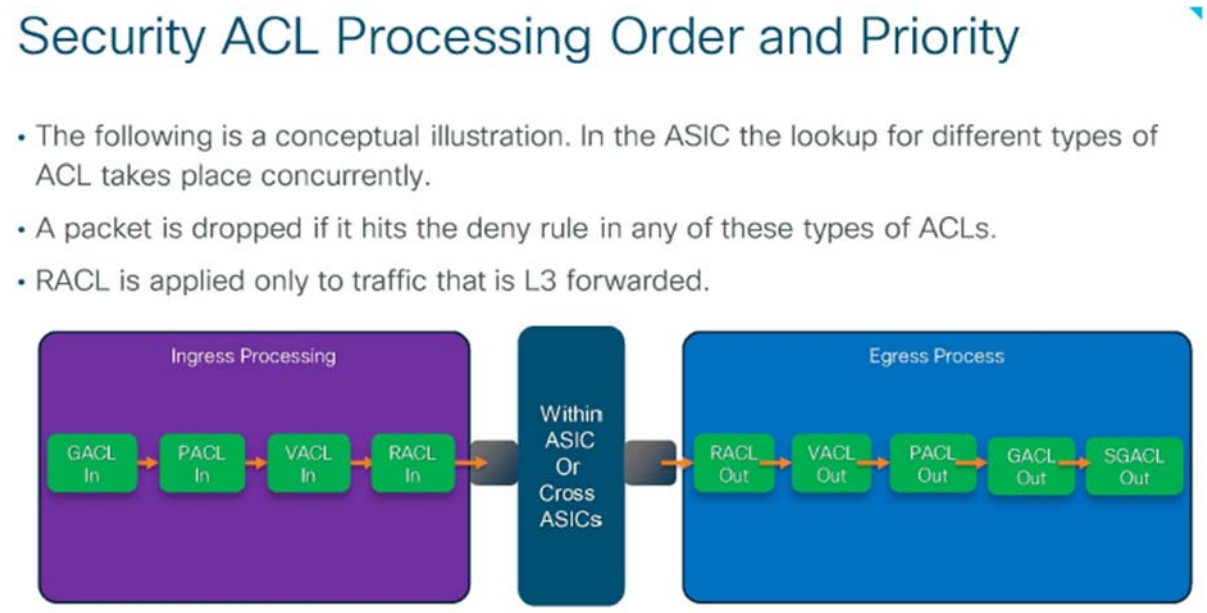
166. The Catalyst 9000 Switch and ISR/ASR Router will automatically block traffic with rapid threat containment when a threat is discovered. Tr. 527:18-530:24; PTX-1326 at 11.

(e) drop each packet in the first portion of packets; and

167. The Catalyst 9000 Switch and ISR/ASR Router will drop packets that are tagged as not being allowed to transfer data to a particular network. Tr. 536:20-539:14; PTX-1390 at 86; PTX-1276 at 216.

168. The Catalyst 9000 Switch and ISR/ASR Router will drop packets that are associated with a deny rule in the ACL because the host has been quarantined. Tr. 537:15-539:5; PTX-1390 at 86; PTX-1276 at 216.

169. The excerpt from PTX-1390 at 86, shows how a packet is dropped (*i.e.*, blocked) if it hits a deny rule:



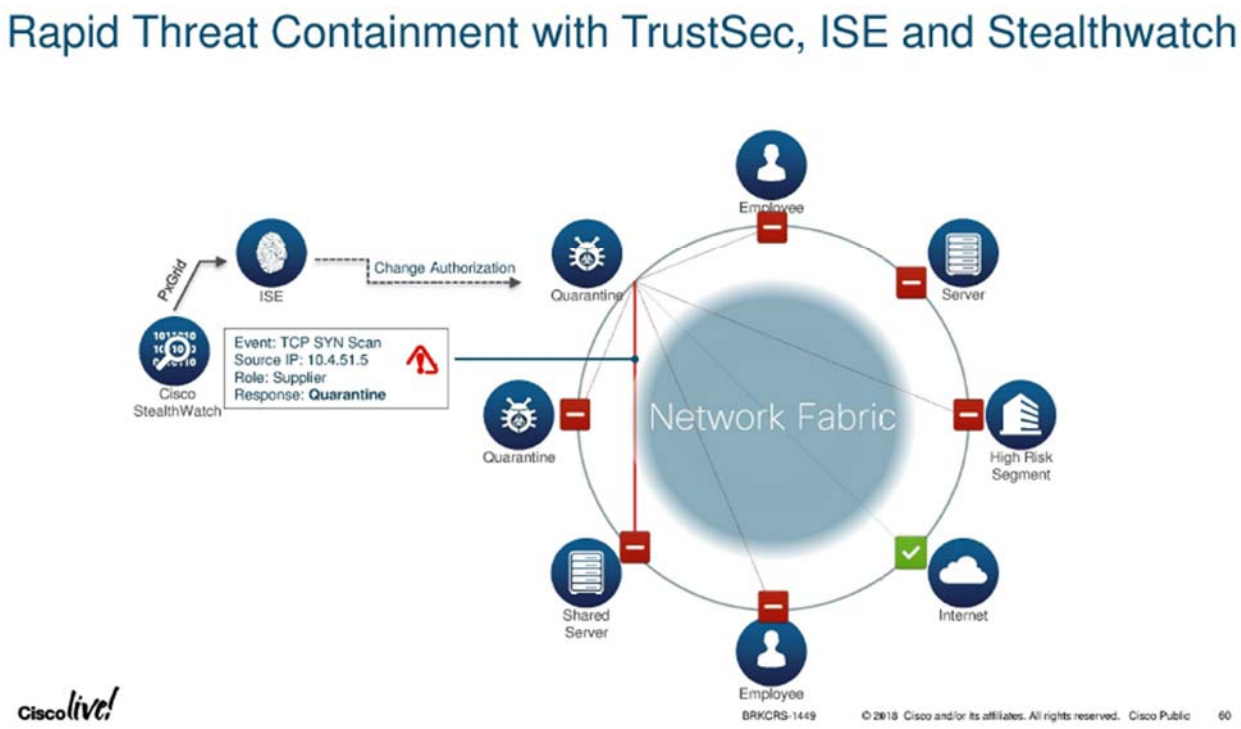
PTX-1390 at 86.

> **(f)** ***responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network: apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and forward each packet in the second portion of packets toward the third network.***

170. The Catalyst 9000 Switch and ISR/ASR Router will allow packets to be sent from devices that are quarantined to certain networks. Tr. 539:17-548:21; PTX-563 at 415; PTX-1288 at 12-13; PTX-1913; PTX-1914.

171. The Catalyst 9000 Switch and ISR/ASR Router will quarantine devices to prevent them from accessing internal networks and other high-risk resources, but will allow the quarantined devices to interact with resources that are not high-risk, such as the Internet and web applications. Tr. 541:9-542:16; PTX-563 at 415.

172. The excerpt from PTX-563 at 415 shows how certain resources are blocked when a device is in quarantine, but those resources in certain other networks, like the Internet (show through the green check) remain available:



PTX-563 at 415.

173. The Catalyst 9000 Switch and ISR/ASR Router will change the permissions of the devices that have been quarantined, but these still include "permits" for resources on different networks that the quarantined device is still able to interact with. Tr. 543:10-544:20; PTX-1288 at 12-13.

174. The Catalyst 9000 Switch and ISR/ASR Router can use a variety of information to enforce its rules. This includes information on the traffic type, application, source, destination, port, and protocol amongst other information. Tr. 782:15-783:12.

175. Dr. Crovella confirmed that the Catalyst 9000 Switch and ISR/ASR Router will block access to certain resources on a network but allow access to other resources on another network when in quarantine. Tr. 2423:19-2424:15.

iii. Doctrine of Equivalents

176. The Catalyst 9000 Switch and ISR/ASR Router perform substantially the same function in substantially the same way, to achieve substantially the same result as the "responsive to" element set forth in the asserted claims. Tr. 549:14-551:20. Substantially the same function as the "responsive to" element is that of making sure that traffic headed toward a specific network will be denied if it is the type that should be stopped. Tr. 550:16-25. It is performed substantially the same way because they use an operator to drop certain packets with a deny mechanism. Tr. 551:1-9. The same result is achieved because the collection of packets is dropped based on the corresponding rule and operator. Tr. 551:10-20.

B. Validity of the '193 Patent

177. Cisco asserts obviousness under 35 U.S.C. § 103 and anticipation under 35 U.S.C. § 102 against the '193 Patent.

178. Cisco asserts Cyber Threat Defense Solution ("CTDS") as the prior art that renders the '193 Patent invalid. DTX-311.

179. Cisco allegedly released and marketed its CTDS sometime in 2012 or 2013. This system was a collection of old Cisco switches and routers, a previous version of ISE, and Lancope's old Stealthwatch. *Compare* Tr. 2430:1-3; DTX-311 with Tr. 2485:5-10; DTX-664 at 4.

180. The CTDS contained an outdated quarantine function that completely isolated a source computer by blocking all packets sent to or from the computer into the network. Tr. 3010:24-3011:9; DTX-711 at 2. With this quarantine functionality, it is impossible to permit data transfers to one network while denying access to another network. Tr. 3011:19-3012:2.

181. The alleged prior art does not mention SGTs or role-based quarantine functionality. *See* DTX-588; PTX-1193.

182. The alleged prior art does not mention application of operators to filter packets based on the attachment of SGTs. Tr. 3015:8-18, 3016:7-21, 3017:1-10; *see also* DTX-588.

183. The alleged prior art does not contain any information showing the application of SGACL to filter packets in the same manner shown by Cisco's technical documents produced after March 12, 2013. *Compare* PTX-1276 at 211, 216 (showing the application of Secure Group Tags and SGACLs by the IOS XE operating system) with PTX-1193 at 7 (showing the same diagram, but failing to make mention of any rules attached and filters based on the application of Secure Group Tags).

184. Cisco's purported CTDS asserted as prior art against the Asserted Claims of the '193 Patent was allegedly made of multiple separate products, consisting of hardware and software and some unnamed Cisco switches and routers, such that they are not a single reference, which is required for anticipation. DTX-311, DTX-588, DTX-711, DTX-1433.

185. Cisco did not show that the combination of the multiple products that make up Cisco's CTDS 1.0 was publicly used or on sale before the effective filing date of the '193 Patent. The earliest date of public availability of Cisco's primary document on the CTDS 1.0 showed a 2014 date. DTX-311 at 85; *see also* DTX-664 at 4; Tr. 3005:21-3006:16.

186. The alleged prior art that Cisco relied upon did not identify reasons or ways one could even combine the prior art to create the same system as the '193 Patent or how the quarantine feature would work. Tr. 3004:1-3005:6, 3008:17- 3010:6.

187. Cisco CTDS is cumulative of the prior art that was considered by the Patent Office during the original prosecution of the '193 Patent and Cisco's IPR petition that was denied by the PTAB (IPR2018-01559). DTX-370 at 13; Tr. 3013:7-3014:9.

188. Cisco used the best prior art in an attempt to invalidate the claims asserted against Cisco in the '193 Patent, but was unsuccessful. Tr. 3013:20-3014:9; DTX-370.

189. Cisco alleged that the technology Centripetal accused of infringement was present in the alleged prior art, however, Dr. Crovella agreed that the Accused Products, such as the Catalyst 9000 Switch, are not reflected in the prior art document that he used. Tr. 2489:21-2490:2.

190. The technology accused of infringing the '193 Patent was not released until June 20, 2017.

191. Cisco's June 20, 2017 press release announcing its unveiling of the network of the future, touted its new family of Catalyst 9000 Switches, which Cisco had "built from the ground up" and that it was "innovating at the hardware (ASIC) and software (IOS XE) layers," informing the world that it built a new kind of product from scratch. PTX-1135 at 946-947; Tr. 3000:9-23.

192. Cisco's Catalyst 9000 Switch represented the "initial build" of Cisco's new intent-based networking capabilities and which provide "highly differentiated advancements in security." PTX-1449 at 884-885.

193. Cisco's CEO stated that Cisco had to "rewrite its IOS to enable its command centre and analytics platform, encrypted traffic analytics, and programmable switches." PTX-1890 at 1.

194. Dr. Striegel provided testimony on the objective indicia of non-obviousness for the '193 Patent, including recognition of the problem, long-felt need in the industry, failure of others, praise by others, industry recognition, copying, and licensing. Tr. 3196:19-3224:16, particularly Tr. 3196:19-3224:16.

195. Dr. Striegel testified about the problem the '193 Patent addressed when he discussed PTX-1113, an Office of Naval Research document that he described as showing a drastically increasing threat space, with attacks increasing in sophistication and the number of devices available to attack increasing. PTX-1113; Tr. 3198:20-3200:19. Dr. Striegel further testified how traditional solutions suffered because they could not handle the increasing volume of data on networks, nor the speed at which attacks changed. Tr. 3200:21-3202:9. Dr. Striegel established that the '193 Patent addressed this because it proactively brought together threat intelligence to combat threats. Tr. 3202:10-3203:12. The '193 Patent's invention provided a solution to the problem of exfiltration that had yet to be solved prior to Centripetal's invention. PTX-460 at 40, 44; Tr. 3198:20-3207:12, 3226:7-13.

196. Dr. Striegel testified that the Asserted Claims of '193 Patent address the network security problem of many network protocols not having security in mind and could be used to exfiltrate data. Tr. 3204:2-21.

197. Dr. Striegel established the long-felt need for the solution of the '193 Patent using PTX-460 at 544. Tr. 3204:22-3207:12. Centripetal's '193 Patent invention addressed the long-felt need in the security field for handling exfiltration. Tr. 235:8-236:19, 343:12-25; PTX-240; PTX-460; Tr. 3205:10-3207:12.

198. There was a failure of others in the industry to provide proactive network protection such as the '193 Patent invention that could scale to larger networks and address emerging threats efficiently. PTX-1113 at 889; Tr. 334:2-15. The existing solutions were reactive, inflexible, and non-scalable and many lacked automation and the inability to use threat intelligence in a meaningful way to live network traffic and use threat intelligence into actionable insight into traffic on the network. PTX-1113 at 889; Tr. 334:2-15.

199. Dr. Striegel established that there was evidence of copying the '193 Patent. Tr. 3223:10-3224:3. Cisco's copying of the invention of the '193 Patent is a secondary consideration of non-obviousness. *See* Findings of Fact, Sections II(C-D), VIII(J), and IX.

200. Dr. Striegel established that there was evidence of licensing the '193 Patent. Tr. 3224:4-3224:16.

201. Centripetal granted a patent license to Keysight Technologies, Inc. ("Keysight") and Ixia ("Ixia") (referred to hereinafter as the "Keysight License"). The Keysight license included a license to the '193 Patent. Tr. 1485:24-1486:14. Some of the patents asserted against Keysight overlap with the patents asserted against Cisco and they were all in the field of network security and operationalizing threat intelligence, further supporting the non-obviousness of the '193 Patent. Tr. 3224:4-16.

202. Cisco, a very large company, has no patent license agreements that relate to functionality of its accused products. Cisco's lack of any patent license agreements relevant to the patented technology is very unusual for such a large company and further demonstrates the non-obviousness of the '193 Patent. Tr. 1477:18-1479:5.

203. Cisco did not present any evidence of the level of skill in the art at the time of the '193 Patent's invention.

204. Cisco did not meaningfully address any secondary considerations. Tr. 2466:13-19.

205. Cisco did not provide any evidence that Claims 18 and 19 of the '193 Patent are invalid under 35 U.S.C. § 101.

206. Cisco did not present any evidence that Claims 18 and 19 of the '193 Patent are invalid pursuant to 35 U.S.C. § 112.

C. Credibility of Witnesses for the '193 Patent

207. Centripetal's technical expert, Dr. Mitzenmacher, relied on twenty-two (22) trial exhibits regarding technical information describing the Catalyst 9000 Switch and ISR/ASR Router technology that was launched in June 2017. *See* PTX-175, PTX-242, PTX-563, PTX-576, PTX-992, PTX-995, PTX-1226, PTX-1260, PTX-1262, PTX-1276, PTX-1280, PTX-1281, PTX-1288, PTX-1303, PTX-1313, PTX-1356, PTX-1409, PTX-1849, PTX-1911, PTX-1912, PTX-1913, and PTX-1914.

208. In its presentation of evidence, Cisco did not cite any technical document produced post June 20, 2017. Instead, Cisco relied on ex post facto animations which were designed for litigation, and do not accurately portray the current functionality of the accused products.

209. Cisco did not call any witness who authored any of the Cisco technical documents relied upon by Centripetal in their infringement case.

210. Cisco's technical expert for the '193 Patent, Dr. Crovella, took positions that established that his testimony was not credible.

211. Dr. Crovella relied almost exclusively on a litigation-derived PowerPoint presentation with 41 slides to support his opinion of noninfringement of the '193 Patent Asserted Claims at trial. Tr. 2349:10-2417:2.

212. In his entire noninfringement trial testimony, Dr. Crovella refers to just one Cisco technical document, PTX-1276, dated 2014. Tr. 2387:18.

213. Dr. Crovella did not point to any Cisco trial exhibit concerning the Catalyst 9000 Switch or ISR/ASR Router that was launched in 2017. Indeed, for much of his testimony, he provided testimony describing why Stealthwatch did not infringe the '193 Patent, but Stealthwatch was not accused of infringing the '193 Patent. Tr. 2407:24-2416:5.

214. During cross-examination, Dr. Crovella admitted that the Catalyst 9000 Switches and ISR/ASR Routers would block some communication between networks but allow others, rebutting his own non-infringement position. Tr. 2423:19-2424:15.

215. Dr. Crovella applied different claim constructions for purposes of invalidity and non-infringement. *See* Tr. 2482:10-25 (testifying that his invalidity opinion was based on "the way that Centripetal interpreted them [the claims]," and that he did not analyze whether the claims were valid over his interpretation of the claims from his non-infringement opinion).

216. On several occasions, the Court called into question the veracity of Dr. Crovella's PowerPoint slides. Tr. 2352:3-2353:6 (manipulating the claim language); 2361:8-18 (mischaracterizing Centripetal's position); 2448:4-2449:16 (questioning the data flow on the slides).

VI. FACTS RELATED TO INFRINGEMENT AND VALIDITY OF THE '806 PATENT

217. The '806 Patent was referred to as the "Rule Swap Patent" at trial. Tr. 572:19-22.

218. The application for the '806 Patent was filed on January 11, 2013. JTX-2.

219. The '806 Patent was issued on December 1, 2015. JTX-2.

220. The priority date of the '806 Patent is January 11, 2013. JTX-2.

221. The '806 Patent expires on December 10, 2033. JTX-2.

222. The Asserted Claims of the '806 Patent are Claim 9 and Claim 17. Dkt. No. 411 at 2. Claim 9 and Claim 17 are, respectively, a system and computer readable media claim.

223. Claim 9 is laid out below:

> A system comprising:
> a plurality of processors; and
> a memory comprising instructions that when executed by

> at least one processor of the plurality of processors cause the system to: receive a first rule set and a second rule set; preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;
>
> configure at least two processors of the plurality of processors to process packets in accordance with the first rule set; after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;
>
> process, in accordance with the first rule set, a portion of the plurality of packets; signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and
>
> configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set: cease processing of one or more packets; cache the one or more packets; reconfigure to process packets in accordance with the second rule set;
>
> signal completion of reconfiguration to process packets in accordance with the second rule set; and
>
> responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

JTX-2.

224. Claim 9 is identical to Claim 17 in every respect except that Claim 17 is a computer readable media claim. JTX-2. Claim 17 substitutes the introductory language of Claim 9, replacing "[a] system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to[.]" JTX-2. For purposes of infringement, the parties addressed the preambles of Claims 9 and 17 separately and the remainder of the claim limitations at the same time. *See* Tr. 573:18-634:14.

225. Dr. Moore, one of the inventors of the '806 Patent, defined the technology in the '806 Patent as a process by which a network device could perform a live swap of rules without sacrificing any security concerns or dropping packets. Tr. 338:19-339-2.

226. CTI is often changing, so the rules that are embedded in the Catalyst 9000 Switch and ISR/ASR Router need to be continually updated. Tr. 339:3-12. Therefore, the rules that are being applied need to be continually swapped out from old rules to new rules. Tr. 339:13-340:1. The most efficient way to do this is by swapping rules while live traffic is going through the device and without any packets being dropped. *Id.*

A. Infringement of the '806 Patent

i. Overview of Infringement for Catalyst 9000 Switches and ISR/ASR Routers

227. Centripetal accuses Cisco's Catalyst 9000 Switch and ISR/ASR Router with DNA Center of infringing Claims 9 and 17 of the '806 Patent. *See* PTX-1263 at 179 (highlighting Cisco's intent-based networks) (2019 document).

228. Cisco compiles source code for the accused switches, routers, and firewalls in the United States. Tr. 462:4-463:18, 464:4-14; PTX-1409 at 5-6. The Accused Products have a plurality of processors and computer memory that stores software instructions. Tr. 573:8-575:6, 642:4-647:11.

229. Cisco uses all of its products, including Cisco's Catalyst 9000 Switch and ISR/ASR Router with DNA Center and Cisco's Firewalls with FMC to protect its own networks in the United States. Tr. 1668:20-1671:10.

230. Cisco's DNA is the management structure that allows the system to take in or utilize threat intelligence, operationalize it, and apply rules and policies that Cisco's Catalyst 9000 Switch and ISR/ASR Router use for security purposes. Tr. 450:23-451:24.

231. The DNA receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to Cisco's Catalyst 9000 Switch and ISR/ASR Router. Tr. 575:15-577:8, 579:18-580:24, 584:14-585:4, 586:15-587:18, 588:12-589:18, 2571:12-2573:8; PTX-992 at 2; PTX-1294 at 3, 15 (2019 document); PTX-1385 at 18.

232. Similar to the DNA, FMC's Threat Intelligence Director (TID) component receives rule sets from various sources and preprocesses the rule sets to create optimized policies which are distributed to Firewalls. Tr. 655:10-656:20, 673:21-675:5, 680:11-681:10; PTX-1289 at 1594; PTX-1293 at 668; *see* Tr. 2537:3-7, 2539:11-17.

233. When new rules are available and sent to Cisco's Catalyst 9000 Switch and ISR/ASR Router by the DNA, they perform a rule swap without dropping any packets. Tr. 597:10-601:8, 606:15-608:14, 633:24-634:14; *see also* Tr. 2571:12-2573:8; PTX-1915; PTX-1195 at 1, 3-4.

234. Similarly, when new rules are available and sent to the accused Firewalls from the FMC, they will perform a rule swap without dropping any packets. PTX-1196 at 1, 7; Tr. 694:22-696:12, 698:8-22, 705:15-707:1.

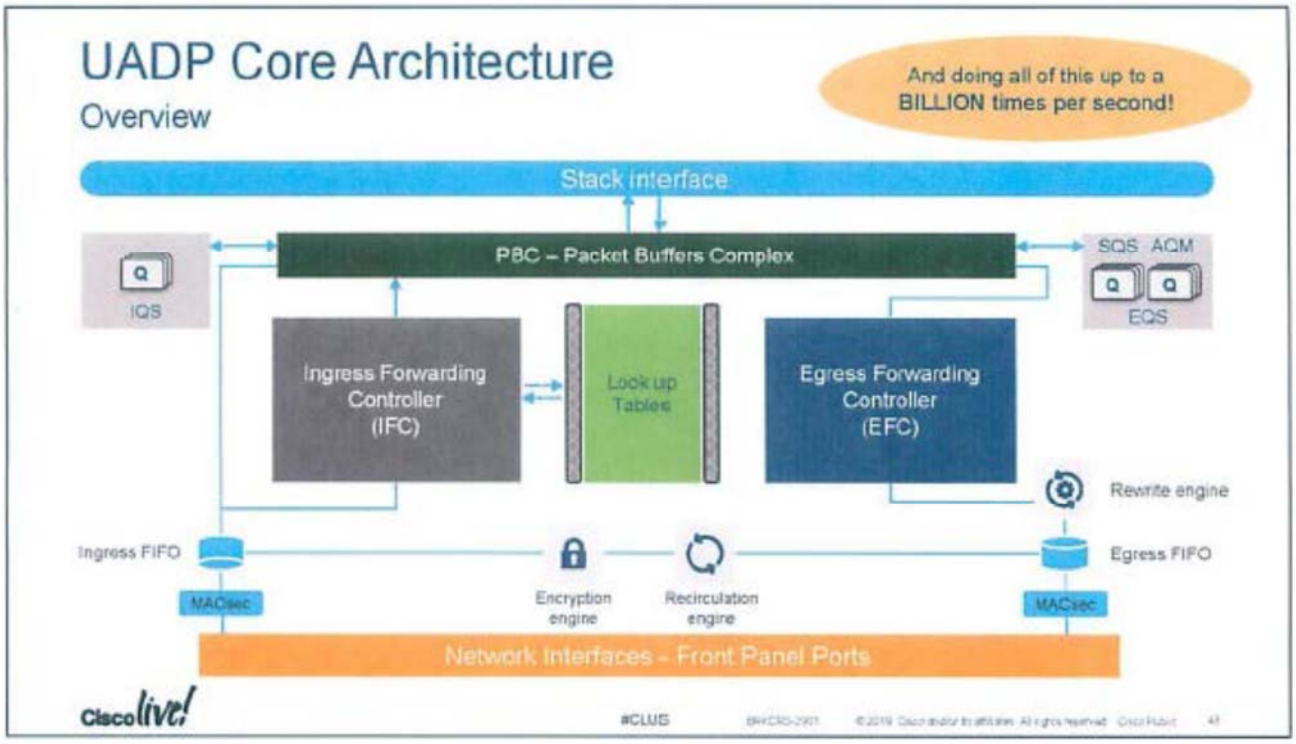
235. Mr. Peter Jones, a distinguished Cisco engineer responsible for building the switching, routing, and enterprise network, explained in detail how the Accused Products process packets and swap rules. Tr. 2543:7-11, 2561:20-2562:1.

236. During cross-examination, Mr. Jones admitted that the Catalyst 9000 Switch infringed every element of claim 9 of the '193 Patent. Tr. 2571:12-2573:8.

237. Mr. Jones was one of the architects for the design of the UADP processer used by Cisco's Catalyst 9000 Switches and ISR/ASR Routers which is a processor that was specifically built in order to provide packet analysis and security. Tr. 2549:2-10. He also provided multiple

technical presentations regarding the operation of the UADP at many Cisco events. *See* DTX-562 at 6.

238. Mr. Jones explained that the architecture that enables packet processing functionality within the switch and/or router is the UADP processor. Tr. 2562:8-18; DTX-562 at 43. The figure below shows the core architecture in detail:



DTX-562 at 43.

239. Mr. Jones noted that as packets arrive into a router and/or switch, they enter through the front panel ports and head into the Media Access Control Security ("MACSec"). Tr. 2567:15-25. The MACSec serves as an encryption block. Tr. 2567:22-23.

240. The packet then moves into the Ingress FIFO (First in First Out). The FIFO, is a buffer that serves to order packets as they enter the device. Tr. 2567:23-2568:3.

241. After the FIFO, the payload of the packet is then sent to the Packet Buffer Complex (PBC) for storage. Tr. 2568:4. Simultaneously, the header and address of the packet is sent to the Ingress Forwarding Controller. Tr. 2563:22-2564:2, 2568:1-11.

242. The Ingress Forwarding Controller processes the packet by matching the header information to a variety of ACLs that are stored in the look-up tables. Tr. 2568:10-16. Based on those ACLs, the Ingress Forwarding Controller then decides to either drop the packet or transmit it forward. *Id.*

243. Mr. Jones explicitly noted that if the packet is to be forwarded, it is sent to the Egress Forwarding Controller. Tr. 2568:17-24. He highlighted that the Egress Forwarding Controller operates identically to the Ingress Forwarding Controller. Tr. 2568:21-24. Therefore, for a second time on exit, the payload of the packet is sent to an egress Packet Buffer Complex while the header is sent to the Egress Forwarding Controller. Tr. 2568:21-24; PTX-1390 at 86.

244. It is in the Egress Forwarding Controller that the packet headers are again compared to ACLs that are located in the look-up tables. Tr. 2568:21-24. On egress, the packet can be dropped or further transmitted. *Id.*; PTX-1390 at 86.

245. If the packet is transmitted by the Accused Products, it goes through an Egress FIFO, an Egress MACSec, and then out of a port on those devices. Tr. 2569:1-4.

246. Mr. Jones noted that the UADP operates on its own fixed time pipeline, meaning there will be a packet processed every two or four internal clock periods. The internal clock periods are not set to a normal time scale, but operate in milliseconds. Tr. 2554:22-24.

247. The Accused Products contain a new FED 2.0 Hitless ACL update. Tr. 2550:18-25. Mr. Jones testified that before the 2.0 Atomic Hitless feature was added to the Accused Products, performing rule swaps often resulted in a discard of a number of packets because rules

would be changed while packets were being processed. Tr. 2552:18-23. Therefore, the new 2.0 Hitless version updated the products so that new ACLs can be placed into the device and be activated without displacing packet processing. Tr. 2551:2-5; PTX-1303 at 73.

248. Below is a description of the older ACL Process:

2.1 Current ACL Change Flow

Currently whenever there is a change to the ACE in an ACL, the data will drop packets during the change to hardware programming.

This is the sequence of events today:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
   a. Create new Policy to use temporarily
   b. Generate a new VMR list
   c. Merge and Optimize new VMR list
   d. Write the Drop Policy label to every LE attached to the old Policy
   e. Remove existing TCAM entries
   f. Overwrite old Policy with new Policy in SDK
   g. Delete new Policy
   h. Write new TCAM entries
   i. Validate which will write the Policy label back into all LE attached to Policy
   j. Return SUCCESS

On ERROR returned from writing entries into TCAM:

- If TCAM is full then leave with Drop Policy label programmed (UNLOADED)
- Display UNLOADED or ERROR message to console to indicate hardware was not programmed with new Policy
- Drop all packets for this protocol type, in this direction on the interface
- Return ERROR

PTX-1195 at 3.

249. Below is a description of the new 2.0 Hitless ACL Update:

2.2 Hitless (Atomic) ACL Change Flow

For this new feature Hitless (Atomic) ACL Change, no packets should drop while programming the new TCAM entries. To allow this to happen a new policy will be created and attached to the interface before deleting the existing policy.

This will always be enabled for all features that set the flag acknowledging support for hitless acl change; and is only available to features that go through ACL common code.

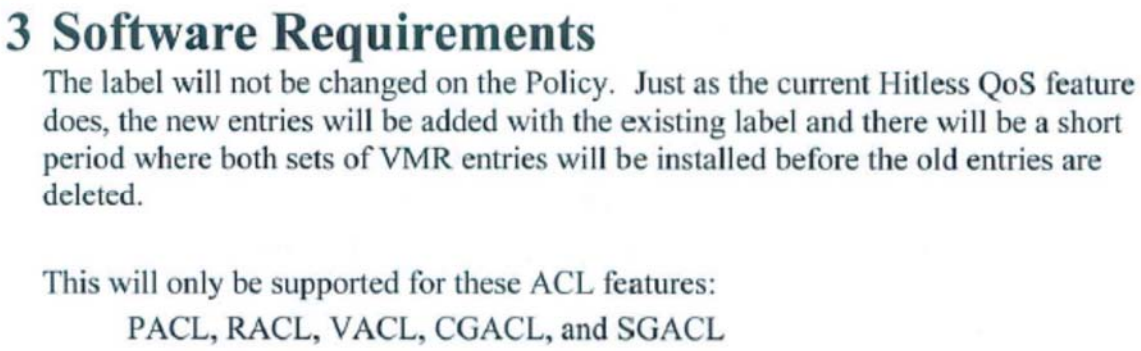
This is the new sequence of events:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
5. Generate a new VMR list
6. Merge and Optimize new VMR list
7. Verify if feature supports hitless ACL change
   - If supported, continue to Step 8
   - If not, use old method starting at Section 2.1 step 4d
8. Add new VCUs into hardware
9. Add new TCAM entries
10. Delete old entries from TCAM
11. Return SUCCESS

On ERROR returned from either of the new steps 7 or 8 will cause it to go back to use the old method of programming described in Section 2.1 starting with step 4d. So then, it will no longer be hitless.

PTX-1195 at 4.

250. In Cisco's software technical specification, the requirements of the software dictate that "there will be a short period where both sets of VMR ["Virtual Media Recorder"] entries will be installed before the old entries are deleted." *See* PTX-1195 at 4. Here is a copy of those software requirements:



3 Software Requirements

The label will not be changed on the Policy. Just as the current Hitless QoS feature does, the new entries will be added with the existing label and there will be a short period where both sets of VMR entries will be installed before the old entries are deleted.

This will only be supported for these ACL features:
PACL, RACL, VACL, CGACL, and SGACL

PTX-1195 at 4.

251. ACLs are sent to the accused switch or router from a variety of sources - including Cisco's Digital Network Architecture (DNA). Tr. 2571:12-17. In order to use the rules, the switches and routers must compile them. Tr. 2571:18-21. Accordingly, DNA begins the process by signaling the accused switch or router to perform a swap from old to new ACLs. Tr. 2572:14-17.

252. While the ACLs are being compiled within the accused switches and routers, they use the old rule set to process packets. Tr. 2571:22-2572:1. After compilation is finished, these devices signal the processor to begin processing packets with the new updated ACL rule set. Tr. 2572:2-6.

253. This swap of ACL rules within the accused routers and switches occur when the processor signals that packets are stored in cache and that no packets are being processed which happens in the middle of the two to four clock cycles. Tr. 2572:7-13. Accordingly, there is a period where the VMR contains both sets of new and old rules will be installed before the old rules are cleared. *See* PTX-1195 at 3-4.

254. After the swap is complete, the accused routers and switches perform a memory write and shows a return success function to the end user. Tr. 2573:5-8.

255. After the return is complete, packets are then processed with the newly updated second rule set. Tr. 2572:14-17.

256. Cisco's expert did not cite any technical document produced post June 20, 2017. Cisco's expert witness relies on animations, produced ex post facto, which were designed for litigation and do not accurately portray the current functionality of the Accused Products. DTX-562, which was altered from its original form as cited by Cisco's employee Mr. Jones, had emphasis added to it to exclude egress from the presentation of Cisco's expert Dr. Reddy.

257. Cisco did not call any witness who authored any of the Cisco technical documents relied upon by Centripetal in their infringement case.

258. Cisco directed its customers because to use the Accused Products as they were described in Cisco's documents, including marketing material, manuals, and source code.

259. Cisco was at least aware of the '806 Patent and the manner its customers infringed the '806 Patent when Centripetal filed the complaint in this case naming the '806 Patent, the Accused Products, and described the manner in which the Accused Products were used to infringe.

ii. Element-by-Element Analysis for Catalyst 9000 Switch and ISR/ASR Router

(a) A system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:

260. The Catalyst 9000 Switch and ISR/ASR Router are computer systems with processors and memory. Tr. 573:18-575:6 (referencing Tr. 473:3-485:13; PTX-1303 at 56; PTX-175 at 598-99; and PTX-1313 at 18).

(b) receive a first rule set and a second rule set;

261. DNA receives rules and threat intelligence that is passed down as rule sets to dynamically update rules on the ISR/ASR Routers and Catalyst 9000 Switches. Tr. 575:7-583:7, 584:14-585:13; PTX-1263 at 179; PTX-1315 at 7; PTX-1294 at 3; PTX-992 at 2.

262. PTX-1294 at 3 is a document created by Cisco that shows that DNA will design a network by creating policies that it provisions to the Catalyst 9000 Switches and ISR/ASR Routers:

Improving your Network from a Single Control and Command Center

Cisco® DNA Center is the foundational controller and analytics platform at the heart of Cisco's intent-based network for large and midsize organizations. Cisco DNA Center provides a single dashboard for every fundamental management task to simplify running your network. With this platform, IT can respond to changes and challenges faster and more intelligently.

- **Design:** Design your network using intuitive workflows, starting with locations where your network devices will be deployed. Users of Cisco Prime® Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) can simply import existing network designs and device images into Cisco DNA Center.
- **Policy:** Define user and device profiles that facilitate highly secure access and network segmentation based on business needs. Application policies allow your business-critical applications to provide a consistent level of performance regardless of network congestion.
- **Provision:** Use policy-based automation to deliver services to the network based on business priority and to simplify device deployment. Zero-touch device provisioning and software image management features reduce device installation or upgrade time from hours to minutes and bring new remote offices online with plug-and-play ease from an off-the-shelf Cisco device.

PTX-1294 at 3.

263. DNA receives updates to its threat intelligence from Stealthwatch and Stealthwatch sends and receives updates to threat intelligence. Tr. 576:10-580:24, 582:24-583:7, 584:14-585:4; PTX-1263 at 179; PTX-1315 at 7; PTX-1294 at 3; PTX-992 at 2.

(c) preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;

264. DNA will preprocess the threat intelligences rules for the Catalyst 9000 Switch and ISR/ASR Router to create rules that are performance optimized for use in the Catalyst 9000

Switch and ISR/ASR Router. Tr. 585:14-591:22, 592:24-595:4, 595:17-23; PTX-1294 at 15; PTX-1385 at 18; PTX-1348 at 5; PTX-1849 at 185.

265. The Catalyst 9000 Switch and ISR/ASR Router will dynamically create and adjust policies through DNA, which are collections of rules, by optimizing the threat intelligence for network and device specific implementations. Tr. 586:15-587:18, 593:20-595:4; PTX-1294 at 15; PTX-1849 at 185.

266. PTX-1294 at 15 is a document created by Cisco that shows that DNA will take threat intelligence rules and create device specific policies:

Policy creation	Allows the creation of policies based on business intent for a particular part of the network. Users can be assigned policies for the services that they consume, and these policies follow them throughout the network. Policies are translated by Cisco DNA Center into network-specific and device-specific configurations that can be adjusted dynamically based on network conditions. Of foundational importance for intent-based networking, policies define the business intent that is desired and allow the network to guarantee services.

PTX-1294 at 15.

267. The Catalyst 9000 Switch and ISR/ASR Router will dynamically update and change from one rule set to another rule set. Tr. 588:12-591:22; PTX-1385 at 18; PTX-1348 at 5.

(d) configure at least two processors of the plurality of processors to process packets in accordance with the first rule set; after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets; process, in accordance with the first rule set, a portion of the plurality of packets;

268. The Catalyst 9000 Switch and ISR/ASR Router use processors to process packets using their rule set and then will reconfigure their processors using the FED 2.0 Hitless ACL technology to process packets according to a new updated rule set. Tr. 595:24-615:15; PTX-1195 at 3-4; PTX-1288 at 12; PTX-1915 ; PTX-1920; PTX-175 at 598.

269. The FED 2.0 Hitless ACL technology improves upon the previous technology used in Cisco's switches and routers because it does not drop packets during a rule set update, while the old technology would drop packets during such an update. Tr. 597:13-602:3, 606:15-608:9; PTX-1195 at 3-4; PTX-1915.

270. PTX-1195 at 4 is a document created by Cisco that describes the new process for continuing to process packets with a policy, then swapping in a new policy, and processing subsequent packets:

2.2 Hitless (Atomic) ACL Change Flow

For this new feature Hitless (Atomic) ACL Change, no packets should drop while programming the new TCAM entries. To allow this to happen a new policy will be created and attached to the interface before deleting the existing policy.

This will always be enabled for all features that set the flag acknowledging support for hitless acl change; and is only available to features that go through ACL common code.

This is the new sequence of events:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
5. Generate a new VMR list
6. Merge and Optimize new VMR list
7. Verify if feature supports hitless ACL change
   - If supported, continue to Step 8
   - If not, use old method starting at Section 2.1 step 4d
8. Add new VCUs into hardware
9. Add new TCAM entries
10. Delete old entries from TCAM
11. Return SUCCESS

PTX-1195 at 4.

271. During processing, the rule sets are stored in Ternary Content-Addressable Memory (TCAM), with new rules being entered and old rules being deleted. Tr. 600:11-605:16; PTX-1195 at 4; PTX-1288 at 12.

272. The Catalyst 9000 Switch and ISR/ASR Router include multiple processors in multicore processors, flow processor, and UADP. Tr. 609:21-614:17; PTX-175 at 598; PTX-1849 at 336.

(e) ***signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:***

273. The Catalyst 9000 Switch and ISR/ASR Router will signal its processors to initiate a change of the rule sets being used to process the packets. Tr. 615:17-24, 616:9-619:14; PTX-1195 at 4; PTX-1916.

274. The Catalyst 9000 Switch and ISR/ASR Router will signal this change over when verifying that the hardware is ready for a switch over to occur to add the new rules into the rule set in the TCAM in hardware. Tr. 616:19-617:18; PTX-1195 at 4.

275. The Catalyst 9000 Switch and ISR/ASR Router will perform a rule swap into the TCAM memory to reprogram the operation of the processors. Tr. 618:7-619:12; PTX-1916.

276. The reprogramming with two- to four-clock cycles in response to a signal to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set. Tr. 2571:12-2573:8.

(f) ***cease processing of one or more packets; cache the one or more packets;***

277. The Catalyst 9000 Switch and ISR/ASR Router will stop the processing of packets while in the process or updating the rule set and will use a memory buffer to cache the packets that are received during the update. Tr. 619:16-629:8; PTX-1390 at 29; PTX-1313 at 62; PTX-1917 at 26:13-22.

278. The accused switch uses the ASIC packet buffer to cache the packets in memory while swapping rule sets in an update. Tr. 621:1-622:8; PTX-1390 at 29.

279. The accused router uses the dispatcher packet buffer to cache the packets in memory while swapping rule sets in an update. Tr. 623:2-625:18; PTX-1313 at 62.

(g) ***reconfigure to process packets in accordance with the second rule set; signal completion of reconfiguration to process packets in accordance with the second rule set; and responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.***

280. The Catalyst 9000 Switch and ISR/ASR Router will reconfigure the processors to process packets according to the new rule set that has been swapped in, and will send a notification when processing can begin again using the new rule set. Tr. 629:9-634:14, 635:14-640:24; PTX-1303 at 73; PTX-1195 at 4; PTX-1288 at 12; PTX-1915; PTX-1849 at 29, 236.

281. The Catalyst 9000 Switch and ISR/ASR Router will update the rules in the ACL and store them in the TCAM after a swap and then use the ACL with the updated rule set. Tr. 632:18-633:9, 637:1-639:25; PTX-1288 at 12; PTX-1849 at 29, 236.

iii. Overview and Element-by-Element Analysis for Firewalls

282. Additionally, Centripetal accuses Cisco's Firewalls with FMC of infringing Claims 9 and 17 of the '806 Patent. *See* PTX-1291 at 7.

(a) ***A system comprising: a plurality of processors; and a memory comprising instructions that when executed by at least one processor of the plurality of processors cause the system to:***

283. The Firewalls include multiple processors and memory to store its application that the processor executes to operate the products. Tr. 643:12-647:11; PTX-244 at 937; PTX-1277 at 7.

(b) receive a first rule set and a second rule set;

284. The Firewalls receive rule sets and updated rule sets from the Threat Intelligence Director (TID) software that is integrated into the Firewall Management Center (FMC). Tr. 647:12-656:20, 660:12-669:10; PTX-1291 at 7; PTX-1289 at 1593-595; PTX-1849 at 91, 132.

285. The TID receives and processes threat intelligence feeds to operationalize these rules for use in the Firewalls. The FMC sends rule set updates based on the processed threat intelligence to the Firewalls. Tr. 651:11-656:20, 661:14-664:23, 667:1-668:21; PTX-1291 at 7; PTX-1289 at 1594; PTX-1849 at 91, 132.

286. Cisco engineer Hari Shankar testified during cross examination that TID creates new rules based on threat intelligence that are sent to the firewall. "(Q. So when the Threat Intelligence Director, after ingesting this threat intelligence sends down the rule to the firewall, the firewall can take action to monitor, block or partially block or no action at all, correct? A. That is correct."). Tr. 2537:3-7.

287. The threat intelligence received by the TID in the FMC includes block rules, where a packet triggering that rule is deemed as being harmful and the packet will be dropped. Tr. 664:24-666:25; PTX-1849 at 91; Tr. 2537:3-7.

(c) ***preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;***

288. The TID in the FMC takes the threat intelligence indicators and preprocesses them into observables that the FMC sends to the Firewalls. The observables are updated as needed in new rule sets. Tr. 669:11-679:10; PTX-1289 at 1594; PTX-1393 at 9; PTX-1918; PTX-1849 at 139.

289. The Firewall uses rules that have been processed by the TID to be into the "observable" format that can be used by the products. Tr. 670:18-672:20, 677:20-678:22; PTX-1393 at 9; PTX-1849 at 139.

290. PTX-1289 is a Cisco technical document that describes the function of TID:

Cisco Threat Intelligence Director (TID) Overview

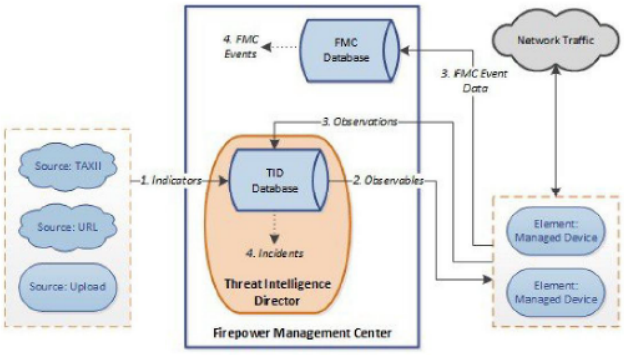
The Cisco Threat Intelligence Director (TID) operationalizes threat intelligence data, helping you aggregate intelligence data, configure defensive actions, and analyze threats in your environment. This feature is intended to supplement other Firepower functionality, offering an additional line of defense against threats.

When configured on your hosting platform, TID ingests data from threat intelligence *sources* and publishes the data to all configured managed devices (*elements*.) For more information about the hosting platforms and elements supported in this release, see Platform, Element, and License Requirements, on page 1500.

Sources contain *indicators*, which contain *observables*. An indicator conveys all of the characteristics associated with a threat, and individual observables represent individual characteristics (e.g. a SHA-256 value) associated with the threat. *Simple indicators* contain a single observable, and *complex indicators* contain two or more observables.

Observables and the AND/OR operators between them form an indicator's *pattern*, as illustrated in the following examples.

Figure 43: Firepower Management Center Data Flow



When a TID incident is fully or partially realized, the system takes the configured *action* (monitor, block, partially block, or no action). For details, see Factors That Affect the Action Taken, on page 1521.

PTX-1289 at 1593-1594.

(d) configure at least two processors of the plurality of processors to process packets in accordance with the first rule set; after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets; process, in accordance with the first rule set, a portion of the plurality of packets;

291. The Firewall configures its processors with the rule set received from the FMC using their transactional-commit model. The Firewalls will process the packets according to this rule set until it receives and updates with the new rule set according to this transactional-commit model. Tr. 679:11-696:21; PTX-1293 at 668-69; PTX-1241 at 253; PTX-1849 at 64, 93; PTX-408 at 822-33.

292. The rule set is compiled in the Firewall to prepare it for use in the rule engine. Tr. 684:23-685:13; PTX-1241 at 253.

293. The transactional-commit model is used by the rule engine in the Firewall to implement changes to the rule set without dropping packets, which is an upgrade from the old model that would drop packets when rules were swapped. Tr. 680:11-682:8, 688:25-690:6, 690:21-692:5, 692:21-693:16; PTX-1293 at 668-69; PTX-1849 at 64, 93.

(e) signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:

294. The Firewalls send a signal to its processors when the new rule set is ready to be swapped in according to the transaction-commit model. Tr. 696:22-704:14; PTX-1293 at 668; PTX-1196 at 8; PTX-1849 at 64, 93.

295. The Firewalls send the signal when the new rule set has finished being compiled and is ready to be swapped. Tr. 697:8-698:2, 703:3-24, PTX-1293 at 668; PTX-1196 at 8.

296. The transaction-commit model used in the Firewall is an upgrade that avoids packet drop and reduces compilation time. Tr. 698:8-703:2; PTX-1196 at 8.

(f) cease processing of one or more packets; cache the one or more packets;

297. The Firewalls stop processing packets with its current rule set once it has been signaled that the updated rule set has been compiled and is ready to be swapped in according to the transaction-commit model. The packets will be held in memory during the time that the new rule set is swapped in to be used by the rule engine. Tr. 704:15-708:24; PTX-1196 at 7; PTX-1277 at 7, 12.

298. The Firewalls have memory called a receive ring for holding packets in a cache while the new rule set is being swapped in. Tr. 707:2-708:18; PTX-1277 at 7, 12.

(g) reconfigure to process packets in accordance with the second rule set; signal completion of reconfiguration to process packets in accordance with the second rule set; and responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

299. The Firewalls compile the updated rule set to be swapped into according to the transaction-commit model and used by the rule engine. The Firewalls signal the rule engine to begin processing again when the processors have swapped in the updated rule set. Tr. 708:25-711:21; PTX-1293 at 669; PTX-1241 at 253-54.

300. The Firewalls will swap in the updated rule set without a gap in deleting the old rule set and applying the new one, which is an advantage over the previous operation. Tr. 709:11-25; PTX-1293 at 669.

iv. Doctrine of Equivalents

301. The Catalyst 9000 Switch and ISR/ASR Routers with DNA, and Firewalls with FMC perform substantially the same function in substantially the same way, to achieve substantially the same result as the "preprocessing" element set forth in the asserted claims. Tr. 712:25-714:18. Substantially the same function as the "preprocessing" element is performed by receiving information regarding threats, including actions such as blocking and monitoring, which has the same goal of turning information into rules and reprocess them in a format appropriate. Tr. 713:21-714:3. It is performed substantially the same way because ingests threat information processes it and turns it into observables that are optimized for systems using the rules. Tr. 714:5-12. The same result is achieved because the rule set is passed down where the system puts that rule into use. Tr. 714:13-18.

B. Validity of the '806 Patent

302. Cisco asserts obviousness under 35 U.S.C. § 103 and anticipation under 35 U.S.C. § 102 against the '806 Patent.

303. Cisco asserts the functionality from a previous Cisco switch, the Catalyst 6500, and the Cisco Prime Network Control System as alleged prior art for the '806 Patent. Tr. 3023:20-25.

304. The alleged prior art functionality asserted within the Catalyst 6500 contains the older version of the ACL Update.

305. The ACL Update, within the Catalyst 6500 switch, operates by adding a new ACL in the Ternary Content-Addressable Memory (TCAM) alongside the old ACL, and merging the two lists together. DTX-686 at 1, 37. This process often causes interruptions and packets to be dropped. *See* DTX-686 at 37-38.

306. The ACL Update was updated to the FED 2.0 version in 2017. PTX-1195 at 1; Tr. 3036:12-3037:4. The FED 2.0 Hitless Atomic ACL Update Software Functional Specification shows the differences between the older version and the new 2.0 version. PTX-1195 at 1, 3; Tr. 3039:20-3042:20. The newer version is accused of infringement by Dr. Mitzenmacher within the Catalyst 9000 Switch and ISR/ASR Router. Tr. 3035:16-3036:25.

307. The older version operated by completely stopping the system, eliminating ACLs, merging and replacing those ACLs, then reactivating the processing system. Tr. 3034:21-3035:2. This system resulted in overlap between the old rules and the new rules within the TCAM. This caused packets to be dropped because old ACLs were being applied alongside the new ACLs, causing conflict and disruption. Tr. 3035:3-15, 3040:2-12; *see* PTX-1195 at 3.

308. The 2.0 Atomic ACL Hitless Update modified the process by eliminating the overlap and implementing rapid swap and replacement of the old ACLs with updated ACLs. Tr. 3041:7-18; *see also* PTX-1195 (technical document from July 2017).

309. Cisco Prime Network Control System's Release Notes shows that Cisco Prime Network Control System operated by monitoring and troubleshooting support for a maximum of packets through the 5000 series Cisco Catalyst switch, allowing viability into critical performance metrics for interfaces, ports endpoints, users and basic switch inventory. DTX-525 at 2. The Release Notes for Cisco Prime Network Control System and Dr. Reddy's testimony contains no mention of the preprocessing of rules or allowing switches to receive rules sent by Cisco Prime Network Control System. Tr. 3043:10-24; *See* DTX-525 at 2. There is no evidence that the predecessor 6500 series switch, aided with Cisco Prime, could swap new rules for the old, as opposed to merging old and new rules together.

310. Cisco's CEO announced in June 2017 that its new network intuitive is based on Cisco's Digital Network Architecture, labelling it as its most significant achievement in the last 10 years. Cisco had to completely rewrite 25 years of software in order to develop its DNA Center, which was not made available until August 2017. PTX-1890; PTX-1135; Tr. 3029:17-23.

311. Cisco's expert, Dr. Reddy, omitted any discussion about the "receiving" and "preprocessing" claim elements, nor did he identify any corresponding functionality in the prior art system. Tr. 3042:9-3045:1.

312. The infringing Hitless ACL FED 2.0 was new technology that replaced the prior version and functioned very differently. Tr. 3034:5-3036:2, 3038:1-3041:18, 3086:12-17; PTX-1195 at 3-4.

313. Dr. Orso confirmed that Cisco Prime Network Control System does not have the same functionality as DNA, and Dr. Reddy's analysis did not show that the two products have the same functionality. Tr. 3042:21-3043:9; PTX-1135 at 946-47; DTX-525 at 1-2.

314. Dr. Striegel provided testimony on the objective indicia of non-obviousness for the '806 Patent, including recognition of the problem, long-felt need in the industry, failure of others, praise by others, industry recognition, copying, and licensing. Tr. 3196:19-3224:16, particularly Tr. 3207:13-3211:1.

315. Traditional solutions were unable to address the problem of performing policy updates without affecting device performance. The '806 Patent solved the problem of rapidly swapping massively scaled cyberthreat intelligence policies to live Internet traffic without dropping packets or sacrificing security. Tr. 338:19-340:1; 3207:13-3208:11. The existing solutions were reactive, inflexible and non-scalable. Tr. 321:1-23. Many lacked automation and

the inability to use threat intelligence in a meaningful way to live network traffic and use threat intelligence into actionable insight into traffic on the network, such that there was a failure of others in the industry to provide protective network protection like the '806 Patent. PTX-1113 at 89; Tr. 334:2-15.

316. Dr. Striegel testified about the problem the '806 Patent addressed when he discussed PTX-1113, an Office of Naval Research document that he described as showing a drastically increasing threat space, with attacks increasing in sophistication and the number of devices available to attack increasing. PTX-1113; Tr. 3198:20-3200:19. Dr. Striegel further testified how traditional solutions suffered because they could not handle the increasing volume of data on networks, nor the speed at which attacks changed. Tr. 3200:21-3202:9. The '806 Patent addressed this because it proactively brought together threat intelligence to combat threats. Tr. 3202:10-3203:12.

317. Dr. Striegel explained that the Asserted Claims of the '806 Patent address the network security problem of potentially dropping packets between swapping rules. He explained that the Asserted Claims of the '806 Patent solved this by allowing a rule swap to take advantage of preoptimization. Tr. 3207:13-3208:11.

318. Dr. Striegel established industry praise for the '806 Patent because Centripetal was identified as a "Cool Vendor" in PTX-1122 at 854, which described aspects of the claims. Tr. 3208:12-3211:1. There was industry recognition and praise for the invention of the Asserted Claims of the '806 Patent. Tr. 3207:13-3211:1, 3200:21-3203:22. Gartner recognized Centripetal's patented technology as "unique" and the importance of it being able to "load large indicator datasets," a problem specifically addressed by the '806 Patent. PTX-1122 at 54-55; Tr. 3208:12-3211:1.

319. Cisco copied the invention of the ’806 Patent. *See* Findings of Fact, Sections II(C-D), VIII(J), and IX. Dr. Striegel established that there was evidence of copying the ’806 Patent. Tr. 3223:10-3224:3.

320. Dr. Striegel established that there was evidence of licensing the ‘806 Patent. Tr. 3224:4-3224:16. The Keysight License included a license to the ’806 Patent. Tr. 1485:24-1486:14. Some of the patents asserted against Keysight overlap with the patents asserted against Cisco and they were all in the field of network security and operationalizing threat intelligence, further supporting the non-obviousness of the ’806 Patent. Tr. at 3224:4-16.

321. Cisco, despite its size, has no patent license agreements that relate to functionality of its accused products. Cisco’s lack of any patent license agreements relevant to the patented technology for such a large company is very unusual and further demonstrates the non-obviousness of the ’806 Patent. Tr. 1477:18-1479:5.

322. Cisco did not present any evidence of the level of ordinary skill in the art at the time of the ’806 Patent’s invention.

323. Cisco did not provide any evidence that Claims 9 and 17 of the ’806 Patent are invalid under 35 U.S.C. § 101.

324. Cisco did not meaningfully address any secondary considerations. Tr. 2671:1-8.

325. Cisco did not provide any evidence that Claims 9 and 17 of the ’806 Patent are invalid pursuant to 35 U.S.C. § 112.

C. Credibility of Witnesses for the ’806 Patent

326. Centripetal’s technical expert, Dr. Mitzenmacher, relied on twenty-six (26) trial exhibits regarding technical information describing the new Catalyst 9000 Switch, ISR/ASR Router and DNA Center technology, and Cisco’s Firewalls with FMC. *See* PTX-244, PTX-408, PTX-992, PTX-1195, PTX-1196, PTX-1241, PTX-1263, PTX-1277, PTX-1288, PTX-1289,

PTX-1291, PTX-1293, PTX-1294, PTX-1303, PTX-1313, PTX-1315, PTX-1348, PTX-1385, PTX-1390, PTX-1393, PTX-1849, PTX-1915, PTX-1916, PTX-1917, PTX-1918, and PTX-1920.

327. Cisco's technical expert for the '806 Patent, Dr. Reddy, took positions that established that his testimony was not credible.

328. Dr. Reddy relied almost exclusively on a litigation derived PowerPoint presentation. Tr. 2580:3-2650:13.

329. In his entire noninfringement trial testimony, Dr. Reddy refers to just one Cisco technical document, PTX-1390. Tr. 2622:24-2623:1.

330. Instead of using Cisco technical document, Dr. Reddy prepared litigation derived animations that contradicted Cisco's own documents, and the Court called Dr. Reddy out on the contradiction. Tr. 2615:25-2616:20 (When Dr. Reddy attempted to claim slide 29 was a representation of DTX-562. "THE COURT: "Well, that's a whole different setup.").

331. Dr. Reddy testified that rules were not applied on the ingress and egress of packets in the Catalyst 9000 Switches or ISR/ASR Routers, which was contradicted by the testimony of Cisco's engineer, Mr. Jones (*See, e.g.*, Tr. 2543:7-11, 2561:20-2562:1, 2571:12-2573:8) and Cisco's non-litigation-created documents. *See, e.g.*, PTX-1195 at 3 (describing sequence of events to swap rules); DTX-562 at 43 (showing UADP processor in the Catalyst 9000 Switch and ISR/ASR Router that is used to swap rules).

332. Dr. Reddy created a demonstrative animation that conflicted with Cisco's technical documents and engineers, opining that rules were only applied by the products for packets entering ("ingress") the product and not when exiting ("egress") the product. Tr. 2615:2-2619:13. In actuality, all evidence showed that rules were applied both at the ingress and egress.

Tr. 2568:5-16, 2568:21-24 (Peter Jones, Cisco Distinguished Engineer); DTX-562 at 43 (the exhibit modified for purposes of Cisco's animation).

333. Dr. Reddy testified that he applied different claim interpretations for his invalidity versus non-infringement opinions for the '806 Patent. Tr. 2675:14-2676:15.

VII. FACTS RELATED TO INFRINGEMENT AND VALIDITY OF THE '176 Patent

334. The '176 Patent was referred to as the "Correlation Patent" at trial. Tr. 973:16-18.

335. The application for the '176 Patent was filed on May 15, 2015, as Application No. 14/714,207. JTX-3 at Cover (21),(22).

336. The '176 Patent issued January 31, 2017. JTX-3 at Cover (45).

337. The priority date of the '176 Patent is February 10, 2015. JTX-3 at Cover (63).

338. The '176 Patent expires on February 10, 2035. *See* JTX-3 at Cover (63).

339. The Asserted Claims of the '176 Patent are Claim 11 and Claim 21. Dkt. No. 411 at 2. Claim 11 and Claim 21 are, respectively, a system and computer readable media claim. JTX-3 at 17:6-35, 18:3-19:23.

340. Claim 11 is laid out below:

> A system comprising:
>
> at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:
>
> identify a plurality of packets received by a network device from a host located in a first network;
>
> generate a plurality of log entries corresponding to the plurality of packets received by the network device;
>
> identify a plurality of packets transmitted by the network device to a host located in a second network;
>
> generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

> correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and
>
> responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:
>
> generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and
>
> provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

JTX-3 at 17:6-35.

341. Claim 11 is identical to Claim 21 in every respect except that Claim 21 is a computer readable media claim. Tr. 974:23-975:16. Claim 21 modifies the introductory preamble language of Claim 11 replacing "[a] system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:" with "[o]ne or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:". *Compare* JTX-3 at 17:6-9 *to* 18:63-65. For purposes of infringement, the parties addressed the preambles of Claims 11 and 21 separately and the remainder of the claim limitations at the same time. Tr. 975:9-16, 2238:7-17.

342. Dr. Moore, an inventor of the '176 Patent, describes the technology of the '176 Patent as the development of a system for identifying malware-infected computers through use of correlation. Tr. 340:11-15, 341:3-15.

343. A single communication between two computers on different networks is often broken down into many different segments of packets. Tr. 340:20-341:2. These segments are compared to ascertain if they are a part of the same communications and then the system can

decide that a computer within the network has been communicating with a computer of a cybercriminal. Tr. 341:3-15. Therefore, the correlation technology in the '176 Patent serves as a method to identify computers in a network that have been infected with malware. Tr. 341:18-19.

A. Infringement of the '176 Patent

i. Overview of Infringement

344. Centripetal accuses Cisco's Catalyst 9000 Switch and ISR/ASR Router with Stealthwatch of infringing Claims 11 and 21 of the '176 Patent. Tr. 975:19-21.

345. The Catalyst 9000 Switch and ISR/ASR Router share the same operating system known as IOS XE. Tr. 448:11-450:4; PTX-242 at 816, 817.

346. The Catalyst 9000 Switch and ISR/ASR Router contain processors and memory that stores software instructions. Tr. 477:12-478:14, 484:13-485:3; PTX-1303 at 0056; PTX-1313 at 0018.

347. The Catalyst 9000 Switch and ISR/ASR Router contain processors that function to transmit packets across different external and internal networks. Tr. 477:12-478:14, 484:13-485:3, 977:18-21.

348. Cisco utilizes NetFlow in the Catalyst 9000 Switch and ISR/ASR Router. Tr. 983:10-984:4; PTX-1060 at 008.

349. As packets are transmitted, the Catalyst 9000 Switch and ISR/ASR Router generate NetFlow logs, which are summaries of information from the transmitted packets. Tr. 977:18-25, 984:5-13; PTX-1060 at 0008. NetFlow includes information such as the source and destination IP address, the source and destination port, and the protocol being used. Tr. 984:5-13; PTX-1060 at 0008.

350. The Catalyst 9000 Switch and ISR/ASR Router are capable of generating NetFlow records for packets at both the ingress into the device and on egress out of the device.

Tr. 986:12-987:1; PTX-1060 at 0023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress); PTX-572 at 762; *see also* Tr. 988:12-22 (Dr. Cole explaining PTX-572 showing "[w]hen you configure a flow record, you are telling the device to show all of the flow data traffic that enters" -- which is ingress – "or leaves" -- egress – "the device.").

351. These NetFlow records are sent up to Stealthwatch, which by 2018 was embedded with Cognitive Threat Analytics (CTA), that digests the information from the ingress and egress NetFlow records. Tr. 998:3-17; PTX-1009 at 0009. Stealthwatch with CTA also has the functionality to be sent data from proxy sources using another type of logging called Syslog. PTX-1065 at 0005 (noting the Stealthwatch "solution uses the Proxy ingestion feature to consume Syslog information . . ."); Tr. 1115:4-116:13. Customers may use either NetFlow or Syslog data or both within Stealthwatch. PTX-1065 at 0005.

352. Stealthwatch correlates NetFlow and/or Syslog information sent by devices on the network to provide a detailed overview of all traffic that is occurring on the network. PTX-1065 at 0005. CTA, working within Stealthwatch, can leverage the correlations of NetFlow telemetry to detect malicious threats to the security of the network. PTX-1009 at 0009; PTX-591 at 522 (using identical language to PTX-1009 in the Stealthwatch Release Notes); *see also* Tr. 997:7-12 ("'telemetry' is just another word for the NetFlow log information. So the NetFlow telemetry, the NetFlow logs, these are all synonymous terms, so this is another way of referring to logs").

353. In response to these correlations, Stealthwatch creates a baseline of normal traffic behavior within the network and based on these normal patterns and known threat indicators, Stealthwatch employs a funnel of analytical techniques to detect advanced threats. PTX-569 at 272; PTX-584 at 402.

354. Stealthwatch, in response to suspicious activity or threats, provisions rules to proactively stop that threat. Tr. 1002:4-1003:21; PTX-1089 at 1238 (showing the use of the Adaptive Network Control (ANC) to implement rules). The ANC operates by applying new policies and changing individual user's authorization on the network according to rules and policies in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:4-19, 1006:19-1007:5; PTX-989 at 0033; PTX-1018 at 0011.

355. Cisco uses all of its products, including Cisco's Catalyst 9000 Switch and ISR/ASR Router with Stealthwatch to protect its own networks in the United States. Tr. 1668:20-1671:10.

356. Cisco directed its customers because to use the accused products as they were described in Cisco's documents, including marketing material, manuals, and source code.

357. Cisco was at least aware of the '176 Patent and the manner its customers infringed the '176 Patent when Centripetal filed the complaint in this case naming the '176 Patent, the accused products, and described the manner in which the accused products were used to infringe.

ii. Element-by-Element Analysis

(a) A system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:

358. The Catalyst 9000 Switch and ISR/ASR Router are systems with processors and memory, where the memory will store instructions that are executed by the processors for operation. Tr. 976:11-977:12 (referencing analysis for the '856 Patent, citing Tr. 913:14-919:15; PTX-524 at 303; PTX-573 at 851-852; PTX-1008 at 0004).

(b) identify a plurality of packets received by a network device from a host located in a first network; generate a plurality of log entries corresponding to the plurality of packets received by the network device; identify a plurality of packets transmitted by the network device to a host located in a second network; generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

359. The Catalyst 9000 Switch and ISR/ASR Router receive packets that are sent between hosts on two different networks, including packets that are received from the first host (*i.e.*, ingress) and that are transmitted by the product (*i.e.*, egress) to the second host. The Catalyst 9000 Switch and ISR/ASR Router will create logs with log entries corresponding to this packet traffic and send them to Stealthwatch. Tr. 977:13-993:18; PTX-408 at 650; PTX-1060 at 0008, 0023; PTX-572 at 762; PTX-569 at 272; PTX-1849 at 243.

360. The Catalyst 9000 Switch and ISR/ASR Router log packet traffic at the ingress and egress in a format called Netflow, which includes information corresponding to the packets in the form of the source and destination IP, the source and destination port, and the protocol (referred to as the 5-tuple data) of the packet. Tr. 982:6-15, 983:10-984:13, 989:20-990:8; PTX-1060 at 0008, 0023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress); PTX-569 at 272; PTX-408 at 650.

361. PTX-408 a screenshot of a document created by Cisco, shows at 650 how policy and flow monitoring is performed at both the egress and ingress:

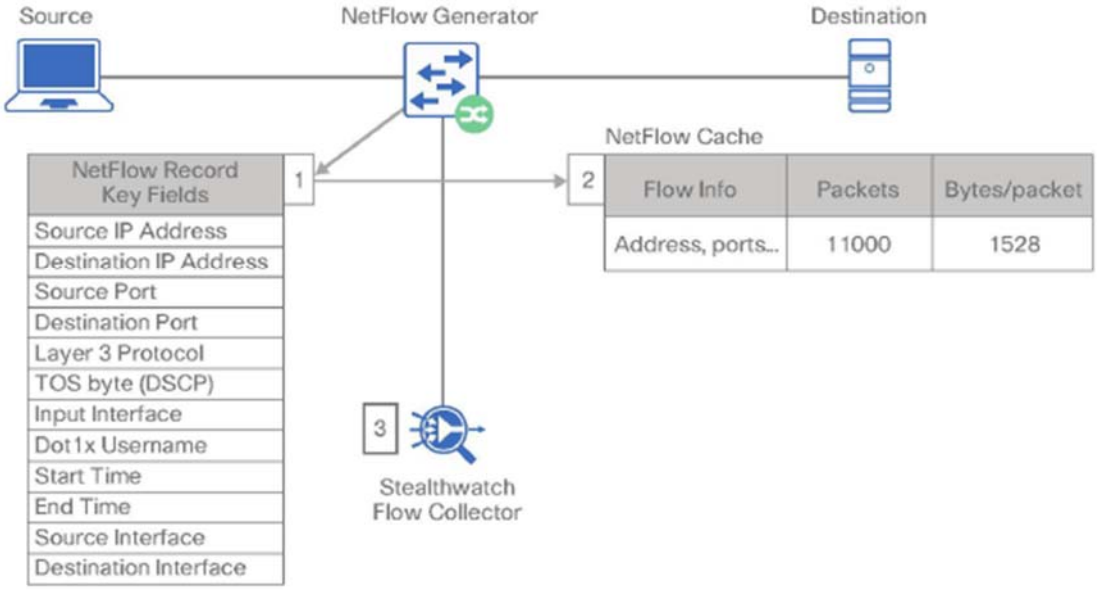
2. Specify the **Egress** and **Ingress** details for the following:

- QoS SSID Policy
- QoS Client Policy
- Flow Monitor IPv4
- Flow Monitor IPv6

PTX-408 at 650.

362. PTX-1060 is a Cisco document that describes at 0008 how the Catalyst 9000 Switch and ISR/ASR Router identify packets associated with a particular flow between a source and a destination and sends the packet data as Netflow to Stealthwatch:

Figure 2 *NetFlow operation on a network device*



PTX-1060 at 0008.

363. The Catalyst 9000 Switch and ISR/ASR Router will send Netflow logs that it generates to Stealthwatch so that Stealthwatch can analyze them. Tr. 987:15-21, 988:12-989:1; PTX-572 at 762.

364. Bidirectional Netflow is captured (packets both sent and received between hosts), as discussed in the Cisco document PTX-569 at 282, which states that "[a]ny interface that is

missing inbound or outbound traffic is not configured properly . . . [and in the example] all are reporting inbound and outbound traffic":

- For each exporter the interface status document shows which interface is reporting traffic using NetFlow. Any interface that is missing inbound or outbound traffic is not configured properly. Any interface not showing here is not sending NetFlow. In the example below 16 interfaces are NetFlow configured. Notice that all are reporting inbound and outbound traffic.

PTX-569 at 282 (*see also* PTX-569 at 272; Tr. 980:23-981:15).

(c) correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and

365. The Catalyst 9000 Switch and ISR/ASR Router will send the Netflow logs they generate to Stealthwatch, which will correlate the packet data from packets received and transmitted by the Catalyst 9000 Switch and ISR/ASR Router. Tr. 993:19-999:15; PTX-1065 at 0005; PTX-591 at 522; PTX-1009 at 0009.

366. Stealthwatch will collect Netflow records and will correlate the traffic data that was collected by the Catalyst 9000 Switch and ISR/ASR Router to identify threats in the network. Tr. 994:21-995:21; PTX-1065 at 0005.

367. PTX-569 is a 2018 Cisco document that demonstrates how Stealthwatch uses NetFlow for correlation:

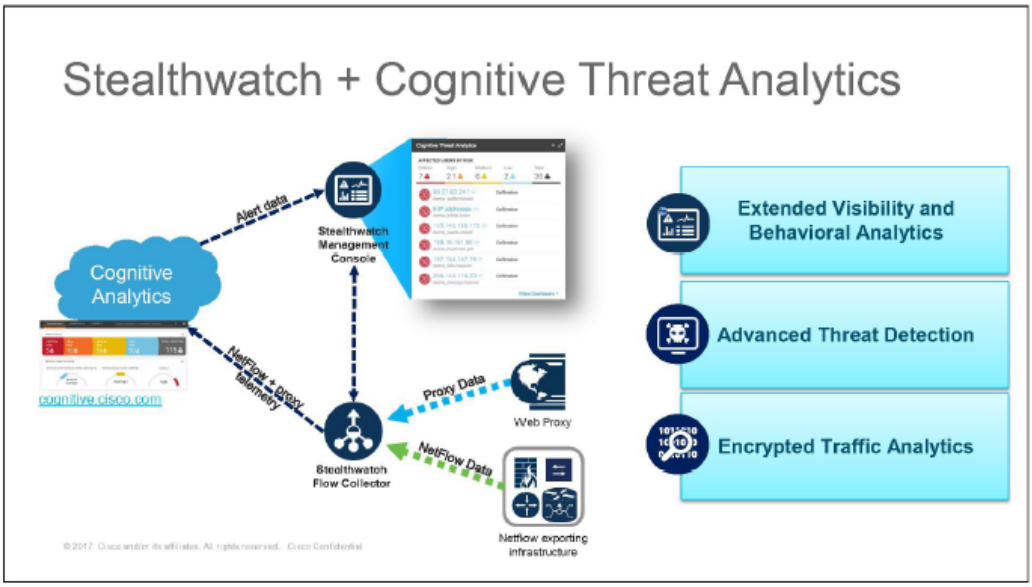
Stealthwatch Enterprise also integrates with a cloud based multi-stage machine learning analytics engine, that correlates threat behaviors seen in the local environment with those seen globally. It employs a funnel of analytical techniques to detect advanced threats.

Figure 3: Detect anomalies and threats

For more information about the Stealthwatch components and architecture, please refer to the Stealthwatch Enterprise Data Sheet.

PTX-569 at 272.

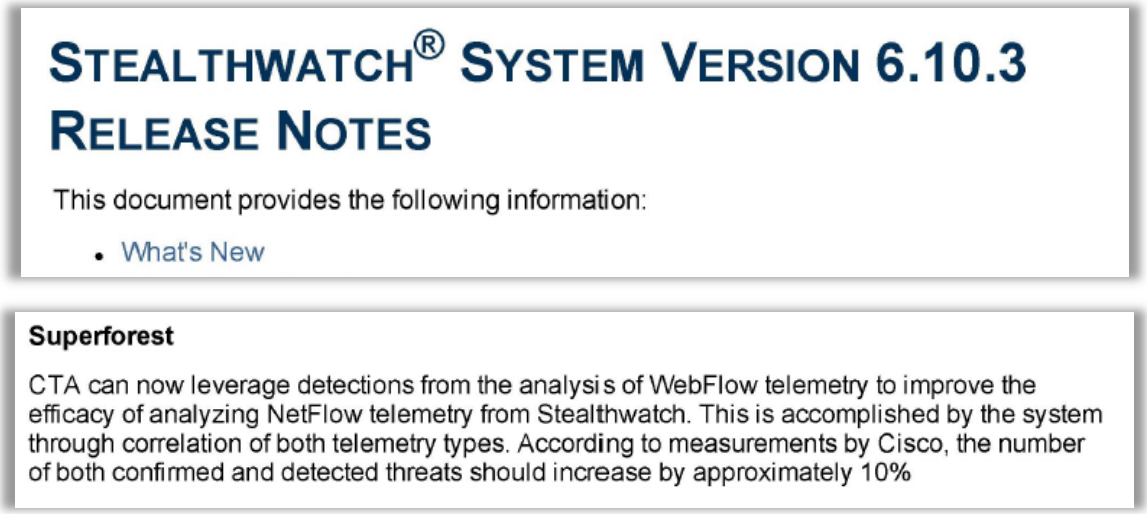
368. PTX-1065 is a document created by Cisco that describes how Netflow records are collected and correlated, noting that it "correlates threat behavior seen in the enterprise with those seen globally":



Stealthwatch integrates with Cognitive Analytics ("CA" – aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

PTX-1065 at 0005.

369. Stealthwatch was upgraded with Cognitive Threat Analytics (CTA) in 2018 order to allow correlation logs from multiple data sources to improve identification of threats. Tr. 996:17-998:17; PTX-591 at 522; PTX-1009 at 0009.



STEALTHWATCH® SYSTEM VERSION 6.10.3 RELEASE NOTES

This document provides the following information:

- What's New

Superforest

CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types. According to measurements by Cisco, the number of both confirmed and detected threats should increase by approximately 10%

PTX-591 at 519, 522.

370. PTX-1009 is a Cisco document that describes at 0009 that CTA can correlate the logs from Netflow records, along with information other information such as WebFlow telemetry:

- CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types. According to measurements by Cisco, the number of both confirmed and detected threats should increase by approximately 10%.
- Example: This is an incident triggered by a malicious domain, which was part of an indicator of compromise (IOC) detected in the WebFlow telemetry.

PTX-1009 at 0009.

371. CTA uses the Netflow records that include bidirectional flow and ingress and egress data and correlates this packet data with WebFlow for the indicator of compromise with the Netflow logs. The Netflow logs will include bidirectional flow data from one machine and will include ingress and egress data from multiple machines. Tr. 980:23-981:15; PTX-1009 at 0009; PTX-569 at 272; Tr. 2278:16-20 (Dr. Almeroth confirming the claim can be based on "one or more" devices).

(d) responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device: generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

372. Stealthwatch will respond to identified threats to generate rules that are sent to the Catalyst 9000 Switch and ISR/ASR Router to block specific packets that were identified to be

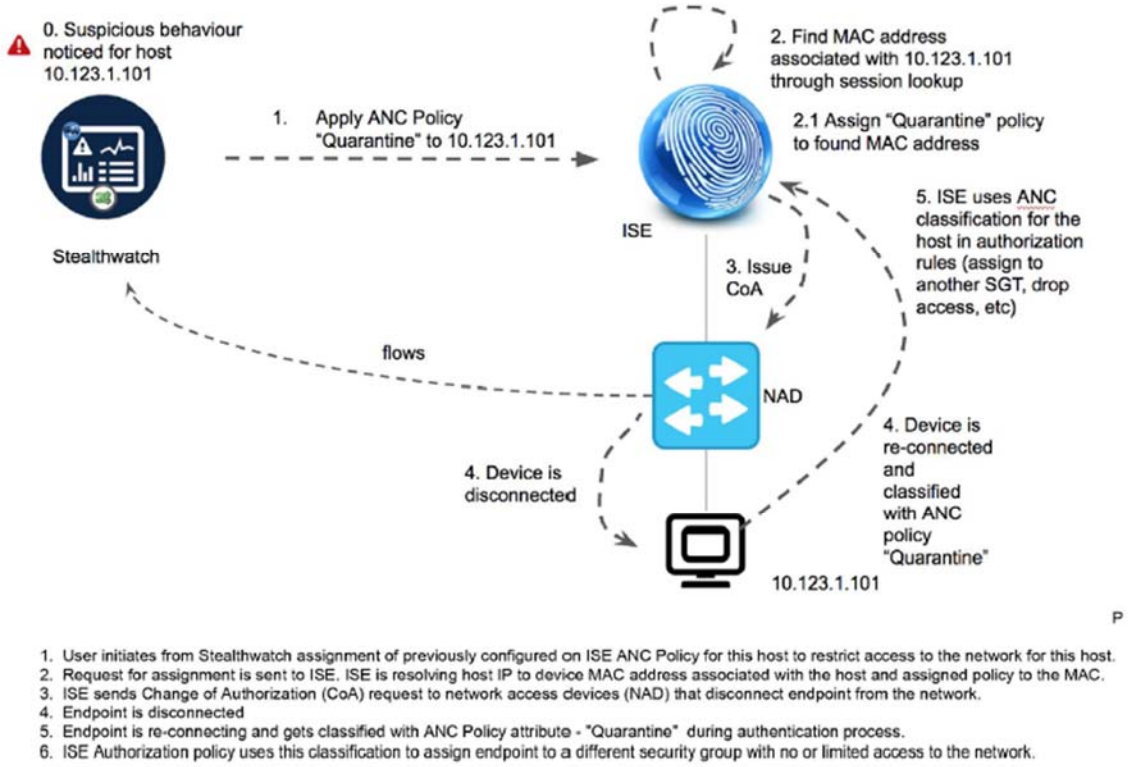
threats. Tr. 1000:2-1007:19; PTX-1849 at 007; PTX-1089 at 0979, 1238; PTX-595 at 179; PTX-1018 at 0011.

373. PTX-1018 is a document created by Cisco that describes CTA:

PTX-1018 at 011.

374. The rules sent to the Catalyst 9000 Switch and ISR/ASR Router are used to identify specific packets through the IP address of the host sending or receiving the packets. Tr. 1002:4-1003:1; PTX-1089 at 1238.

375. PTX-1089 is a document created by Cisco that describes at 1238 that the policy will be sent to quarantine:



PTX-1089 at 1238.

376. Stealthwatch was upgraded in Stealthwatch 7.0 (2019) to include "Change Mitigation Actions" using ANC policies to initiate quarantines. Tr. 1005:4-19; PTX-595 at 179; PTX-1089 at 1238 ("Initial ANC Integration (Stealthwatch 7.0 release) will be done by integrating using pxGrid 1.0 SDK.").

B. Validity of the '176 Patent

377. Cisco asserts obviousness under 35 U.S.C. § 103 and anticipation under 35 U.S.C. § 102 against the '176 Patent.

378. Sometime in 2012 or 2013, Cisco allegedly released and marketed CTDS. This system was a collection of old Cisco switches and routers, prior version of ISE, and Lancope's old Stealthwatch. Tr. 2304:10-20, 2308:11-23.

379. Cisco asserts its CTDS, using an older version of Stealthwatch, as the prior art that renders the '176 Patent invalid. DTX-311; DTX-312; DTX-343; DTX-463 (all documents from pre-2017).

380. The Stealthwatch version asserted as prior art is version 6.5.4 ("Old Stealthwatch"). Tr. 2344:20-22. This version of Stealthwatch incorporated Stealthwatch Labs Intelligence Center ("SLIC") threat intelligence information, which contained human collected threat indicators. Tr. 3153:2-19; DTX-312 at 1-2.

381. Old Stealthwatch was able to respond to alarms generated by worms, viruses and internal policy violations. DTX-463 at 014 (noting Stealthwatch responds to alarms). There is no indication in the pre-2017 documents that Stealthwatch issued rules in response to correlations of NetFlow.

382. Cisco Stealthwatch incorporated Cognitive Threat Analytics in Stealthwatch in 2017. Tr. 2342:4-7. In version 7.0 of Stealthwatch released in 2019, CTA was improved with the ability to leverage threat detection from the analysis of WebFlow, produced by Syslogs, and NetFlow telemetry by correlating the data. PTX-1893 at 011.

383. In response to these correlations, Stealthwatch creates a baseline of normal traffic behavior within the network. Based on these normal patterns and known threat indicators, Stealthwatch, using CTA, employs a funnel of analytical techniques to detect advanced threats. PTX-569 at 272; PTX-584 at 402 (post-2017 documents).

384. Stealthwatch, in response to suspicious activity or threats, provisions rules to proactively stop that threat. Tr. 1002:4-1003:21; PTX-1089 at 979, 1238 (showing the use of the Adaptive Network Control ("ANC") to implement rules). The new ANC, which replaced the old quarantine functionality, operates by applying new policies and changing individual user's

authorization on the network according to rules and policies in response to correlated threats on the network. PTX-595 at 179; Tr. 1005:4-19, 1006:19-1007:5.

385. Dr. Almeroth alleged claims 11 and 21 of the '176 Patent failed written description for "correlation" because some specific technology implementations, like "artificial intelligence," "machine learnings," "Netflow" and "Cognitive Threat Analytics" were not called out in the specification. Tr. 2332:18-2334:17, 2345:1-8.

386. Dr. Jaeger showed that "correlate" and "responsive to correlating" were sufficiently disclosed within the specification of the '176 Patent. Tr. 3155:1-3157:14. Dr. Jaeger described how the specification discloses support "correlate" with a packet correlator that can utilize logs to correlate packets transmitted by network devices by analyzing log entries, including timestamp information. Tr. 3155:11-3156:8; JTX-3 at 8:46-63, 9:24-43. Dr. Jaeger described how the specification discloses support for "responsive to correlation" by disclosing a particular host in the network being defended and provisioning specific rules in response, which include rules for dropping packets. Tr. 3156:20-3157:14; JTX-3 at 3:23-31, 13:14-33.

387. Dr. Striegel provided testimony on the objective indicia of non-obviousness for the '176 Patent, including recognition of the problem, long-felt need in the industry, failure of others, praise by others, industry recognition, copying, and licensing. Tr. 3196:19-3224:16, particularly Tr. 3211:2-3215:3.

388. Dr. Striegel testified about the problem the '176 Patent addressed when he discussed PTX-1113, an Office of Naval Research document that he described as showing a drastically increasing threat space, with attacks increasing in sophistication and the number of devices available to attack increasing. PTX-1113; Tr. 3198:20-3200:16. Dr. Striegel further testified how traditional solutions suffered because they could not handle the increasing volume

of data on networks, nor the speed at which attacks changed. Tr. 3200:21-3202:9. The '176 Patent addressed this because it proactively brought together threat intelligence to combat threats. Tr. 3202:10-3203:12. The existing solutions were reactive, inflexible and non-scalable. Many lacked automation and the ability to use threat intelligence in a meaningful way to live network traffic and use threat intelligence into actionable insight into traffic on the network. PTX 1113 at 89; Tr. 334:2-15.

389. Dr. Striegel explained how the asserted claims of the '176 Patent can address problems when a threat space changes dynamically. The Asserted Claims of the '176 Patent can address this problem by allowing to correlate log entries from different vantage points. Tr. 3211:3-3211:25. There was a failure of others in the industry to provide proactive network protection such as the '176 Patent's invention that could address emerging threats efficiently. PTX 1113 at 889; Tr. 334:2-15.

390. Dr. Striegel established the long-felt need for the '176 Patent using PTX-1112 at 864-865, because it speaks to the need of those to go resolve the problem addressed by the '176 Patent, and specifically called out correlation. Tr. 3212:1-3215:3. The evidence showed long-felt need for the invention of the '176 Asserted Claims. PTX-1112 at 664-65 (Office of Naval Research announcement from 2010 discussing the need for correlation technologies that "required decision support and near real-time network-based asset control with an 'on the fly' engagement capability."); Tr. 3202:10-3203:12, 3211:2-3215:3.

391. Cisco copied the invention of the '176 Patent. *See* Findings of Fact, Sections II(C-D), VIII(J), and IX. Dr. Striegel established that there was evidence of copying the '176 Patent. Tr. 3223:10-3224:3.

392. Dr. Striegel established that there was evidence of licensing the '176 Patent. Tr. 3224:4-16. The Keysight License included a license to the '176 Patent. Tr. 1485:24-1486:14. Some of the patents asserted against Keysight overlap with the patents asserted against Cisco and they were all in the field of network security and operationalizing threat intelligence, further supporting the non-obviousness of the '176 Patent. Tr. 3224:4-16.

393. Cisco, despite its size, has no patent license agreements that relate functionality of its accused products. Cisco's lack of any patent license agreements relevant to the patented technology for such a large company is very unusual and further demonstrates the non-obviousness of the '176 Patent. Tr. 1477:18-1479:5.

394. Cisco did not present any evidence of the level of skill in the art at the time of the '176 Patent's invention.

395. Cisco did not meaningfully address any secondary considerations, including the long-felt need for the '176 Patent's invention and failure of others to achieve the invention. Tr. 2331:16-2332:9.

396. Cisco did not provide any evidence that Claims 11 and 21 of the '176 Patent are invalid under 35 U.S.C. § 101.

397. Cisco only discussed "correlate" and "responsive to correlating" in Claims 11 and 21 of the '176 Patent as being relevant to 35 U.S.C. § 112.

C. Credibility of Witnesses for the '176 Patent

398. Centripetal's technical expert, Dr. Cole, relied on fifteen (15) trial exhibits regarding technical information describing the new Catalyst 9000 Switch, ISR/ASR Router and Stealthwatch technology. *See* PTX-134, PTX-408, PTX-547, PTX-569, PTX-572, PTX-591, PTX-595, PTX-1009, PTX-1018, PTX-1046, PTX-1060, PTX-1065, PTX-1089, PTX-1849, and PTX-1930.

399. Cisco's technical expert for the '176 Patent, Dr. Almeroth, took positions that established that his testimony was not credible.

400. Dr. Almeroth relied almost exclusively on a litigation derived PowerPoint presentation to support his opinion of noninfringement of the '176 Patent. Tr. 2210:4-2277:9. During cross examination, Dr. Almeroth admitted that his slide that he relied on to show how the accused system allegedly operates (slide 22) was not based on any Cisco technical document, but instead was created for this litigation. Tr. 2281:6-17.

401. In his entire noninfringement trial testimony, Dr. Almeroth refers to a few trial exhibits that Dr. Cole introduced, and proceeds to testify that Dr. Cole got it incorrect. Dr. Almeroth opined that Dr. Cole's infringement opinion relied on the systems' use of logs provided by Cisco's proprietary logging technology, NetFlow, as the logs outlined by the claim language. Dr. Almeroth construed the claims to require identification and generation of logs out of the same network device on ingress and egress. Tr. 2249:1-9, 2250:8-9, 2259:8-22, 2275:24-2276:2. Therefore, Dr. Almeroth avers that the Cisco system cannot infringe, because in his opinion, the Catalyst 9000 Switches and ISR/ASR Routers do not generate NetFlow on both ingress into a device and egress out of one network device. Tr. 2249:1-18. On cross examination, Dr. Almeroth conceded that his single device construction is incorrect. Tr. 2278:11-20. Moreover, Cisco's technical documents refute Dr. Almeroth's conclusion. Dr. Cole pointed directly to PTX-1060, a Cisco technical document dated December of 2017, showing that the Catalyst switches have the ability to export NetFlow on ingress and egress. Tr. 986:12-987:1; PTX-1060 at 0023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress). Dr. Almeroth, on cross-

examination, even admitted that the Catalyst 9000 Switches and ISR/ASR Routers can be configured to export ingress and egress NetFlow. Tr. 2286:10-19.

402. On cross examination, Dr. Almeroth contradicted his previous position that Netflow could not be configured on ingress and egress, the crux of his noninfringement position. He walked back his conclusion to instead opine that Stealthwatch produces an error based on producing both ingress and egress NetFlow. To support that claim, Dr. Almeroth relied solely on the presentation of source code from the 6.5.4 version of Stealthwatch that operated without enhanced NetFlow or the integration of Cognitive Threat Analytics (CTA). Tr. 2287:5-19; *see also* DTX-1616 (showing source code from a previous 6.5.4 version of Stealthwatch that is not accused by Centripetal). He cites to no technical document that confirms that the accused/current version of Stealthwatch produces an error when exporting both ingress and egress NetFlow. In fact, the technical release notes for CTA, which was incorporated into Stealthwatch in 2017, support that CTA produced the ability for the correlation of NetFlow telemetry. PTX-1009 at 009.

403. Dr. Almeroth admitted he used a different understanding of the Asserted Claims of the '176 Patent for his Invalidity Opinion than for his Non-Infringement Opinion. Tr. 2340:18-2341:3. He also testified that while the claims would be valid if he applied the same interpretation used for infringement for validity, he was "not offering opinions [for validity] under what [he] believe[s] is the proper claim scope." Tr. 2341:16-23.

404. Dr. Almeroth ignored that rules being generated in response to correlation was a new feature that was not previously included in Stealthwatch. Tr. 2256:3-2257:10. Cisco technical documents contradict his testimony. PTX-569.

VIII. FACTS RELATED TO DAMAGES

405. Centripetal has one term license in its patent portfolio—a 2018 agreement with Keysight Technologies, Inc. and Ixia (collectively, "Keysight") (the "Keysight License"). *See* Findings of Fact, Section VIII(F)-(G).

406. The earliest start date for damages is June 20, 2017, for the Catalyst 9000 Switches and ISR/ASR Routers infringing the '193 Patent, with subsequent start dates tracking the release of subsequent accused products. The parties do not have a dispute regarding the date of the hypothetical negotiation in June 2017. *See* Findings of Fact, Section VIII(K).

407. The Asserted Patents do not expire for many years, extending through 2033 and 2035. Tr. 1480:13-15; JTX-2; JTX-3; JTX-4.

408. The history between the parties relates to their positions at the hypothetical negotiation, the calculation of damages, and consideration of injunctive relief. That history is described in detail in Findings of Fact, Section II(A)-(D) and incorporated herein.

A. Cisco Incorporated Centripetal's Patented Technologies into Its Products, Making, Using, Offering for Sale, Selling, and Importing Them "as a Single System"

409. Cisco makes, uses, and sells all the infringing products as integrated systems providing comprehensive security solutions. The infringing software is embedded in the hardware products, and sold with it, as detailed below.

410. Cisco does not dispute that the infringing products are sold as integrated systems.

411. In June 2017, Cisco unveiled its "network of the future" that "stops security threats in their tracks." *See* PTX-452 (Cisco press release); Tr. 1159:9-1161:5. Cisco's new line of network products integrated security into its switches, routers and firewalls with corresponding management software to generate, process and enforce rules that protect against network threats. *See, e.g.,* Tr. 733:3-734:22 (citing PTX-585 at 410).

412. Cisco's new line of products was sold as a system, called the Digital Network Architecture ("DNA Portfolio") to achieve "***built-in security***" within network devices. *See* Tr. 577:19-578:24 (citing PTX-1315 at 7 (Cisco presentation)); PTX-452. The DNA portfolio is "a portfolio of innovative hardware and software ***designed to work together as a single system***" to "build ***security into*** [Cisco's] network devices" and create a "comprehensive threat defense architecture" with "integrated security." PTX-452.

413. Cisco claimed that "[o]nly Cisco provides a ***single network fabric*** that is powered by deep intelligence and integrated security" and highlighted that Cisco networks are intent-based networks which provide "[p]erimeter-based, reactive security that has been supplanted by network-embedded, content-based security that reaches from the cloud to the enterprise edge." PTX-1263 at 179-80; *see also* PTX-1348.

414. The DNA portfolio includes infringing technologies: Catalyst 9000 Switches and ISR/ASR Routers, Stealthwatch with CTA, and DNA Center. PTX-452 (Cisco press release); PTX-1263 (Cisco document); Tr. 450:23-451:24.

415. These technologies "typically come together as a part of the overall data solution." PTX-1906 (Radhakrishnan deposition testimony) at 8:6-21, 10:11-25, 11:7-9, 11:11-24.

416. Later in 2017, Cisco redesigned its firewalls and released a new version of the Firepower Management Center to add infringing rule swapping functionality. Tr. 655:10-656:20, 673:6-675:5, 679:19-681:11, 694:13-696:12; PTX-1291 (Firepower Release Notes); PTX-1289 (Firepower configuration guide).

417. By launching its "network of the future" with the "built-in security" of Centripetal's technologies, Cisco achieved the differentiation of its switches, routers and

firewalls that it needed to combat commoditization. PTX-1449 (Cisco 10-K; Catalyst 9000 Switches "provide highly differentiated advancements in security"); *see* Findings of Fact, Section II(D)-(E).

418. Indeed, after incorporating Centripetal's technology in its products, Cisco's sales increased. *See* Tr. 2967:13-2973:10 (asserted patent issuance dates), 3435:4-3438:24 (summary of increased revenue calculations).

419. As described below, Cisco identifies infringing software functionalities as embedded and built-in benefits and features of its infringing hardware products.

420. The Catalyst 9000 Switches are "built for security" (PTX-1260 at 849) and embedded with infringing software code. Tr. 53:15-54:20; 61:16-62:5; 477:2-478:14; 890:10-22; 911:21-912:12; PTX-561 at 630; PTX-1303 at 56.

421. The ISR/ASR Routers are similarly designed for security and embedded with infringing software code. Tr. 54:14:55:12; 477:10-478:14; 887:18-888:6; 890:10-22; 911:21-912:12; PTX-561 at 630; PTX-1303 at 56.

422. DNA Center is embedded within Cisco's Catalyst 9000 Switches and ISR/ASR Routers. Tr. 451:3-24, 578:25-580:5; PTX-1294 at 3. Cisco also touts DNA Center as a "feature" and "benefit" of upgrading to these infringing routers and switches. PTX-1507 (Cisco router benefits); PTX-1260 (Cisco white paper).

423. Similarly, Cisco touts Stealthwatch as a "feature" of ISR/ASR Routers, selling Stealthwatch with Catalyst 9000 Switches and ISR/ASR Routers "as one product." Tr. 1463:13-1464:13; PTX-1507 at 495.

424. Cisco's Firewalls are embedded with infringing software code. Tr. 662:15-663:9; PTX-1849 at 91, 93.

425. As Cisco's own expert explained, the infringing products were sold as "a comprehensive technique" and a "***comprehensive set of products***." Tr. 2130:7-20 (Schmidt testifying that "layered defense," such as by combining Stealthwatch and Firewalls, is needed for customers to avoid "having their networks hacked."). Cisco's documents are in accord, including, *e.g.*:

a) Cisco presentation identifying how the infringing products work together as a security solution (PTX-989 at 33);

b) Cisco's webpage showing security benefits of Firewalls with FMC as a package (PTX-197);

c) Cisco's SEC statements that Cisco delivers an integrated "cybersecurity architecture." (Tr. 1453:8-1454:7; PTX-560 at 771 ("By combining a number of security technologies, we are delivering an end-to-end zero trust architecture."); and

d) Cisco whitepaper stating Catalyst 9000 Switches and DNA are "a critical part of an end-to-end integrated security solution" (PTX-1260 at 849).

426. Centripetal's damages expert, Mr. Gunderson, detailed how the infringing products were sold together as a system. Tr. 1459:10-1469:18 (citing Cisco external documents PTX-1248, PTX-1507, PTX-197, PTX-1035, PTX-276). He explained that while "they might have a separate charge . . . they're selling it as one product . . . they're really trying to sell a solution rather than just sell individual products." Tr. 1464:7-13.

427. Cisco Accused Products are embedded with infringing software and directly infringe. Tr. 53:15-55:12; 61:16-62:5; 477:2-478:14; 887:18-888:6; 890:10-22; 911:21-912:12;

PTX-561 at 630; PTX-1303 at 56; *see also* PTX-276 at 865-66 (Cisco marketing Stealthwatch as part of the accused Switches and Routers).

428. Cisco's marketing materials show that it sells DNA and Stealthwatch as "features" of the Catalyst 9000 Switches and ISR/ASR Routers, directly contradicting Cisco's claim it sells them without this functionality embedded. Tr. 1462:5-1464:13, 1472:17-25; PTX-1507 at 494-95.

429. Notwithstanding all the evidence, Cisco claimed there was insufficient proof that its products were sold in the infringing combinations. However, it never identified any credible rebuttal evidence to suggest the royalty base included non-infringing sales. Cisco's damages expert, Dr. Becker, did not support his damage theory that less than 5% of all sales involved infringing combinations.

430. Dr. Becker simply excluded from his proposed royalty base—without support—***all*** revenues from Catalyst 9000 Switches, ISR/ASR Routers, and Firewalls, which is completely contrary to how Cisco offered for sale and sold its infringing products as integrated systems. Tr. at 2937:5-25 (admitting he excluded the Accused Products' revenue from damages for the '193 Patent, where the Catalyst 9000 Switches and ISR/ASR Routers are accused without other products); Tr. at 2938:1-15 (admitting he did not include the Accused Products' revenue for any patent). Moreover, in doing so he excluded from his royalty base the smallest saleable patent practicing unit, *i.e.*, the Catalyst 9000 Switches and ISR/ASR Routers, for at least the '193 Patent for which only the Catalyst 9000 Switches and ISR/ASR Routers were accused.

431. Given the "tremendous" disparity between the parties' damages calculations and Centripetal's unrebutted evidence, the court gave Cisco another opportunity ***after the close of all evidence*** to provide rebuttal evidence that its products were not sold as integrated systems and

demonstrating "what [Cisco] considered to be the relevant products." Tr. 2970:23-2971:4, 2976:11-2977:17. The Court invited Cisco to provide anything "you think would be helpful" because "you're not limited by what I ask for." Tr. 2976:11-2977:17.

432. Despite the Court giving Cisco a second bite at the apple to prove its theory and having several weeks to compile such evidence, Cisco did not produce any compilation of sales figures to support its theory.

B. The Accused Products Are Made, Used, Offered for Sale, Sold, and Imported into the United States, Including for Products Sold Abroad

433. The Accused Products are made, used, offered for sale, and sold in the United States. Tr. 1474:9-17, 1474:18-1475:17; *see also* PTX 1409 at 5-6, PTX 1932.

434. Cisco's foreign sales of the Accused Products are directly tied to Cisco's direct infringement in the United States of making, using, selling, offering for sale, and importing the Accused Products. Tr. 1513:13-1514:11.

435. Cisco admitted that it compiles the source code for the Catalyst 9000 Switches, ISR/ASR Routers, and Firewalls (which are embedded with infringing code, *see* Findings of Fact Section VIII(A)) in the United States. PTX-1409 at 5-6; Tr. 1474:9-1475:19; PTX-1932.

436. Cisco uses and tests the Catalyst 9000 Switches, ISR/ASR Routers, and Firewalls in the United States. *See, e.g.*, Tr. 1658:11-24, 1659:25-1661:22, 1661:23-1662:7 (Cisco's United States-based Senior Director of Incident Command explaining Cisco uses Stealthwatch, CTA, and "quite a few" additional tools in its own network, and Cisco is "one of the first to deploy a new Cisco technology" in general); Tr. 1674:20-22, 1698:6-7 (Cisco's incident response team uses Stealthwatch).

437. Cisco develops, uses, and tests Stealthwatch in the United States. Tr. 462:4-464:19, 1474:9-1475:17 (citing PTX-1932); PTX-1409.

438. Cisco developed, tested, and compiled source code for the ISR/ASR Routers in the United States. PTX-1906 at 74:18-75:10, 76:12-16.

439. FMC and the DNA Center are specifically designed and configured to work with the infringing functionality of the Catalyst 9000 Switches, ISR/ASR Routers, and Firewalls, whose code is compiled in the United States. Tr. 764:17-765:1; PTX-1409.

440. Cisco's worldwide headquarters is in San Jose, California, and Cisco reasonably exercises control and approval over the manufacture, offer for sale, and sale of its products from its headquarters. Tr. 2932:18-2934:1; PTX-1889.

441. Cisco and its customers use the patented technologies in the Accused Products from the United States for places/customers outside the United States. PTX-1409.

442. Eighty-five percent of world internet traffic travels across Cisco's systems. Tr. 1449:15-1450:5.

C. Cisco and Centripetal are Direct Competitors

443. Centripetal and Cisco are direct competitors with respect to the infringing software and firewalls. Both Cisco and Centripetal market and sell firewalls. Although Centripetal does not market and sell switches and routers, Cisco has embedded the patented software functionality from the Asserted Patents into the Catalyst 9000 Switches and ISR/ASR Routers that provide the same functionality as the RuleGATE product. Tr. 53:15-54:20; 1559:22-1560:9.

444. Centripetal, a start-up company, has had notable growth. Tr. 1209:19-1210:4. Centripetal's revenues doubled year-over-year—before flat-lining when Cisco entered the market with the Accused Products. Tr. 1209:19-1210:20.

445. Centripetal sells its products across a wide range of industries to organizations of all sizes, including small and medium business as well as large enterprises and data centers. Tr. 255:15-256:6, 1202:6-22, 1448:22-1449:3.

446. Cisco and Centripetal operate in the same market space of network security. Tr. 264:5-17, 1208:17-1209:15, 1579:25-1582:24.

447. Cisco's customers are of the same type and nature as Centripetal's target customer base, ranging from small business to large corporations, banks, retailers and government agencies. Tr. 1202:6-22, 1331:18-1332:2, 1448:4-1456:2; PTX-560; PTX-333.

448. Centripetal's Vice President of Sales testified that Centripetal has encountered Cisco in the marketplace when selling its solutions. Tr. 1331:15-1332:2.

449. Centripetal has lost customer opportunities to Cisco. Tr. 264:5-17, 1632:23-1633:7.

450. Centripetal learned that in particular client environments where a potential customer already has Cisco's products, it would rely upon Cisco's existing infrastructure rather than a new vendor. Tr. 1331:23-1332:2, 1459:10-24, 1463:2-6; *see* PTX-1248; PTX-1507.

451. Cisco is larger and more prominent than Centripetal, with a broader product offering and more resources and flexibility regarding the terms it can provide to customers. Tr. 1449:15-1450:5.

452. Cisco's relative size and competitive relationship to Centripetal in the same market space negatively impacts Centripetal's ability to sell its patented products and partner with third–party companies. Tr. 264:5-17; 1494:7-17.

D. The Asserted Patents Provide Significant Benefits Over Older Cisco Modes

453. Following a $65 million investment in research and development, Centripetal launched its patent-practicing RuleGATE system and CleanINTERNET service marked with its

patents that collect, process and implement threat intelligence. Tr. 242:13-243:3; 1202:23-1203:19.

454. The technology received a number of awards, such as the Gartner Cool Vendor Award, the Signet 16 Innovators Award, and the FinXTech Labs Award. Tr. 254:24-255:14. Centripetal's technologies secure the networks of customers such as the Department of Homeland Security, the Home Shopping Network, QVC, and NASDAQ. Tr. 255:17-256:6.

455. The Asserted Patents provide the following benefits:

a) The '193 Patent: Cybercriminals use dangerous security breaches called exfiltration attacks to hijack computers on a network and steal ("exfiltrate") data. Tr. 343:12-344:8, 465:16-21. Protecting against these attacks had proven difficult, and counter-measures were crude. Cisco's previous technology identified potentially compromised computers and completely shut down any network traffic to or from those machines (Tr. 3009:16-3010:6), resulting in significant productivity costs. The '193 Patent prevents potentially compromised computers from making a particular type of data transfer, e.g., accessing a company's sensitive data, while allowing other types of data transfers, e.g., accessing the internet. JTX-4 at 7:6-20, 14:9-36; Tr. 39:15-40:4, 343:12-346:15, 467:14-469:9, 1384:12-20.

b) The '806 Patent: Network devices may include rules to monitor and filter network traffic. Because cyber threats evolve rapidly, these rules require frequent updates. Tr. 339:5-340:1. Centripetal recognized that "[a]s rule sets increase in complexity, the time required for switching between them

presents obstacles for effective implementation" and often results in dropping packets. JTX-2 at 1:20-22. The '806 Patent preprocesses rules and performs rule swaps between the processing of packets to ensure none are dropped. JTX-2 at 4:60-64, 11:40-53.

c) The '176 Patent: Centripetal recognized that it could identify malware-infected computers on a network through "correlation" techniques. Tr. 341:3-15. Centripetal's technology analyzes and correlates logs corresponding to network traffic to identify and remediate unusual activity using network security rules. Tr. 973:16-975:16. The '176 Patent increases the utility of otherwise commodity hardware of traditional switches and routers by transforming them into systems that can play a vital role in network security by sensing and reacting to network threats. Tr. at 341:21-342:10; Tr. at 973:19-974:22.

456. As Cisco's technical document detailed, the average cost of a single data breach in 2018 was $3.86 million (PTX-584)—more than Dr. Becker's reasonable royalty for all the Asserted Patents combined—which shows why Cisco's customers paid it over $20 billion dollars for its infringing security products between June 2017 and June 2020. PTX-1629.

457. As described in Sections III, V(A)(i), VI(A)(i), and VII(A)(i) of the Findings of Fact, the Asserted Patents operationalize threat intelligence, which was a sea change in cybersecurity. The Asserted Patents transform raw CTI into computer logic and algorithms that are applied directly to live internet traffic to stop cyber attacks before or as they are occurring, before they cause any damage. Tr. 308:14-309:12.

458. Cisco's acquisition of cybersecurity companies shows that its commoditized predecessor network products needed enhancement by adding Centripetal's patented technologies. In particular, when developing its cybersecurity software system, Cisco repeatedly spent considerable monies to acquire smaller companies that produced software security technology. From 2013 to 2015, Cisco acquired Sourcefire for $2.7 billion, Lancope for $435 million, and ThreatGRID for an undisclosed amount. Tr. 1605:6-15. Combinations of technologies acquired from these companies form the basic elements of the older Cisco technology which preceding the infringing systems. Tr. 1605:6-23.

459. Cisco added the infringing technologies to these underlying older components to become the industry leader it claimed to be. Cisco's technical and marketing documents describe the addition of the infringing functionalities as a "breakthrough" in building "an intelligent platform with unmatched security." PTX-1135; PTX-963.

460. The addition of the infringing software functionality to the older predecessor models of the infringing products resulted in increased revenue for Cisco. Tr. 1607:22-1608:18, 3435:4-3438:24.

461. These increased revenues coincide with the improvements in the hardware itself. The infringing software significantly improved the existing hardware not only by adding Centripetal's security functionalities, but speed and scalability as well. Tr. 2621:5-10, 2634:14-18 (showing how ASICs process packets at high speeds and how Centripetal's rule swap technology aids that process and its disclosed in the '806 Patent); PTX-547 ("Centripetal's patented filter algorithms eliminate the speed and scalability problem.").

E. Cisco Makes Extensive and Valuable Use of the Asserted Patents to Execute on its Business Strategies

462. Leading up to the dates of first infringement, Cisco was concerned about the commoditization of its switches and routers (which was viewed by market analysis as a "major challenge" for Cisco), and needed to differentiate these products. At this time, Cisco told investors that it planned to dedicate resources to security, a "top" priority. Tr. 1450:6-1453:4; 1456:3-1457:8; PTX-1460.

463. By incorporating the technology of the Asserted Patents into the Catalyst 9000 Switches and ISR/ASR Routers, Cisco was able to execute on its goal of avoiding commoditization of those products by differentiating them to provide "end-to-end zero trust" cybersecurity to gain competitive advantage and drive growth. Tr. 1450:6-1458:19, 1491:13-1492:19; PTX-560, PTX-333, PTX-1460.

464. Cisco internally referred to the infringing technologies—and in particular, the infringing combinations as an integrated solution—as valuable and providing the differentiation it needed. Tr. 1469:10-1474:8, PTX-31.

465. Cisco's infringing products are profitable and commercially successful. Tr. 1495:7-1496:19. The gross profits of the infringing products from June 20, 2017 to December 31, 2019 are:

Tr. 1495:7-1496:19.

466. Cisco presented no evidence refuting these figures.

467. Cisco touted the very high profitability of the Catalyst 9000 Switches as compared to older models. Tr. 1472:17-1474:8, 1495:7-1496:22; PTX-515. Cisco reported that the Catalyst 9000 Switches are the "fastest-selling product ever," "propel[ling] the Company's Finances," and had a "meteoric rise since it was launched in June 2017." PTX-515.

468. Cisco presented no evidence of any acceptable non-infringing alternatives for the technology covered by the Asserted Patents. Tr. 1491:13-1492:19, 1602:2-23.

469. Cisco uses the infringing systems itself. Cisco did not dispute that it uses and tests DNA and Stealthwatch with the Catalyst 9000 Switches and ISR/ASR Routers, and FMC with Firewalls. *See, e.g.,* PTX-1906 at 74:18-75:10; Tr. 1661:6-1662:25, 1698:4-14; *see* Findings of Fact, Section VIII(B).

470. Cisco makes its systems and thus infringes the computer readable media and system claims. Findings of Fact, Sections V(A)(i), VI(A)(i), and VII(A)(i).

471. The scope of Cisco's infringement includes all infringing products Cisco made and used—not just sold—which should be included in the royalty base.

472. Cisco did not design around Centripetal's patents, or make any attempts to design a product to avoid infringing Centripetal's patents. Tr. 1081:8-22, 1642:8-13.

473. Cisco did not take precautions to avoid infringement; rather, Cisco modeled its products after Centripetal's technologies. Tr. 1081:8-22.

474. The record evidence identifies no other cybersecurity solutions that offer the same benefits and advantages of the patented technologies. Tr. 1600:24-1602:16.

475. There is no evidence that Cisco had any belief, let alone a good faith belief or opinion of counsel, that the patents were invalid or that its products did not infringe Centripetal's patents.

476. Cisco continues to utilize Centripetal's patented solutions to this day.

F. The Comparable Keysight License Is the Only License Agreement in Evidence

477. Centripetal licensed the Asserted Patents only once – as part of a 2018 agreement with Keysight Technologies, Inc. and its subsidiary, Ixia (collectively, "Keysight") (the "Keysight License"). Centripetal granted Keysight a [redacted]. *See* PTX-1125; Tr. 1479:10-1482:18. Keysight agreed to a royalty rate of [redacted]. PTX-1125; Tr. 1481:4-10. [redacted]

[redacted]. PTX-1125; Tr. 1479:10-1481:18.

478. The Asserted Patents are technologically comparable to Centripetal's patents asserted in the Keysight litigation—namely, the '856 Patent, and U.S. Patent Nos. 9,264,370 ("the '370 Patent"), 9,413,722 ("the '722 Patent"), 9,560,077 ("the '077 Patent"), and 9,565,213 ("the '213 Patent")—because:

a) As a general matter, the Asserted Patents and the patents asserted against Keysight are all in the same technology area of network cyber security and involve network device hardware, software and services that incorporate Centripetal's patented cybersecurity technology. Tr. 1147:24-1150:24, 1159:9-1160:7.

b) The '176, '193 and '806 Patents are in the same patent family and covered similar fields of technology as the patents that were asserted in the Keysight litigation:

(1) The '176 Patent is technically comparable because it is a continuation of the '370 Patent and discloses similar technology to the field of technology disclosed in the patents asserted in the Keysight case, including collecting and correlating packet log entry data. Tr. 1391:24-1392:19.

(2) The '370, '722, '077, and '213 Patents dealt mainly with different forms of rule-based network-threat detection.

(3) The '193 Patent is comparable to the patents asserted in the Keysight litigation because it deals with receiving and processing

packets, and does so using packet-filtering rules that are configured to drop packets associated with a particular type of data transfer, similar to field of the technology of the patents at issue in the Keysight case. Tr. 1391:24-1392:19.

(4) The '806 Patent is comparable to the patents asserted in the Keysight litigation because it discloses a first rule set and a second rule which are used by a network protection device to process packets, which is similar to the field of technology disclosed in the patents asserted in the Keysight litigation. Tr. 1391:24-1392:19.

479. The Keysight License is the only license to the Asserted Patents, and the only license identified by either party as comparable. Cisco did not identify any licenses. Tr. 1476:12-1479:5; 1497:18-1498:10.

480. The [redacted] (for products that directly compete with RuleGATE) is sufficiently comparable to provide a starting point for determining a reasonable royalty based on a hypothetical negotiation in this case. Tr. 1485:24-1486:24.

481. Centripetal and Cisco are direct competitors with respect to the infringing software and firewalls. Tr. 1559:22-1560:9; 1209:19-1210:20; 1491:3-22. Both Cisco and Centripetal market and sell firewalls. Tr. 1174:18-1175:10, 1186:11-1187:12, 1505:12-15; PTX-1111. Although Centripetal does not market and sell switches and routers, Cisco has embedded the patented software functionality from the Asserted Patents into the Catalyst 9000 Switches and ISR/ASR Routers that provide the same functionality as the RuleGATE product. Thus, the

accused Cisco products are more comparable [redacted] in the Keysight License. Tr. 1489:11-1490:2; 1499:6-16.

482. The two royalty rates are on gross revenue of the licensed Keysight products. The running royalty in the Keysight License has a risk-shifting effect, so that the royalty payment is based on Keysight's sales, and that was the value that the parties deemed to give to their products and the patented technology over the term of the license. Tr. 1483-1484.

483. The running royalty amounts are unimpacted by the circumstances of the Keysight License (settling a patent infringement litigation), because [redacted]. Tr. 1481:11-1482:18; 1485:11-17.

484. The Keysight License was executed during trial when the parties had a clear understanding of validity and infringement, which is comparable to the circumstances of the hypothetical negotiation, when the Asserted Patents are assumed to be valid and infringed. Tr. 1482:21-1483:24; 1487:8-1491:2.

485. Mr. Gunderson accounted for the similarities and differences between the Keysight License and the hypothetical negotiation in this case. Tr. 1485:11-1491:2.

486. The timing of the two licenses is comparable, with the hypothetical negotiation occurring in 2017 and the Keysight License negotiation occurring in 2018. Tr. 1487:25-1489:10.

487. The payment structure and duration are comparable, with the hypothetical license imputing a 2.5 year running royalty, and the [redacted]. Tr. 1488:22-1489:10.

488. The Keysight License encompassed Centripetal's entire patent portfolio (whereas the hypothetical license is to the Asserted Patents), but as is common practice, the negotiation

was based on the technologically-comparable patents asserted in the Keysight litigation. Tr. 1487:4-15, 1489:11-1491:2.

489. Both agreements are non-exclusive, negotiated at arms-length and are market-based. Tr. 1489:11-20.

490. The Keysight License's [redacted], but since all the Accused Products are made in the United States, it can capture their worldwide sales. Tr. 1489:11-1491:2.

491. While Centripetal agreed to license its patents once – in the Keysight License – it would prefer to maintain its patent monopoly. Tr. 1477:10-17.

492. The commercial relationship of the parties to the hypothetical negotiation and the Keysight License are comparable, as Centripetal competes with both Keysight and Cisco. Tr. 1490. Keysight and Cisco both offer and sell networking products to customers of the same type and nature, and both sell network device products that incorporate Centripetal patented technologies. Tr. 1246:20-1247:19, 1331:18-1332:2; PTX-560.

493. Cisco's incorporation of the patented functionality into the infringing products would result in substantial lost profits from the RuleGATE product. Tr. 1606:12-1607:21.

494. Cisco would gain substantially from licensing the Asserted Patents, as it could incorporate advanced security functionality into its products, thus improving the profitability of its networking products. Tr. 1494:3-1495:6, 1607:22-1608:18.

495. Neither Cisco nor Keysight had non-infringing alternatives to the Asserted Patents, and [redacted] accounts for this fact. Tr. 1602:5-23.

G. The Keysight License Offers an Already-Apportioned Royalty Rate

496. The Keysight License applies its specified royalty rates to [redacted]. PTX-1125 at 493-494; Tr. 1483:25-1485:4, 1490, 1564:2-21.

497. Mr. Gunderson explained that his reasonable royalty analysis, when compared apples-to-apples with the Keysight license royalty, [redacted]. *Id.*

498. If the base for the hypothetical license is kept the same as in the Keysight license—*i.e.*, [redacted] fully accounts for the differences between the agreement and the hypothetical negotiation.

499. Thus, further apportionment—and specifically, apportionment of the revenue base—is not required.

H. The Royalty Base is Conservatively Apportioned

500. Notwithstanding the apportioned rate in the Keysight License, Centripetal offered evidence apportioning the royalties in its revenue base.

i. Overview of Feature Apportionment

501. As a conservative measure, Centripetal's expert, Dr. Striegel, performed a technical apportionment of the royalty base. Tr. 1338:16-1339:24. He identified each Accused Product's top-level functions of equal technical value ("functions") based on technical information—namely, Cisco's technical documents, depositions, source code and discussions of infringement with Centripetal's other technical experts (Tr. 1337:17-1340:6; PTX-1931)—and used technical data sheets and product overviews to guide his testimony of these "core" functions. Tr. 1340:7-1341:17, 1427:15-1429:2.

502. He distilled Cisco's complex technology into generally-named functions and used some terms that did not appear in these documents, such as "commodity components." Tr. 1344:20-1345:22, 1428:12-1429:2.

503. Dr. Striegel identified functions from each Accused Product. Tr. 1345:23-1347:6; 1405:6-21; PTX-1931.

504. Dr. Striegel separated infringing and non-infringing functions on a patent-by-patent and product-by-product basis for apportionment. Tr. 1375-76, 1401-2; PTX-1931; *see* Tr. 1349. For example, he excluded non-infringing, commodity-type functions, such as life-cycle management, ports, power supplies, cables, maintenance, and operating systems. Tr. 1375:20-1376:16, 1407:1-14, 1429:25-1430:22.

505. Although processors existed previously, Dr. Striegel explained the importance of Cisco's specific new processors, for example, "delivering" the patented technology and their role in infringement. Tr. 1415:8-1416:3. He focused on the patent claims, determining they were a "considerable improvement in technology" and "an altogether new capability" for network security. Tr. 1413:12-22.

506. Dr. Striegel identified "core" functions, *i.e.,* the essential components of each product as perceived by a network and security expert with an extensive engineering background. Tr. 1409:16-25, 1427:23-1429:24. Dr. Striegel relied on Cisco documents providing "a representation of what Cisco viewed as being important" and "what Cisco represents to their customers." Tr. 1414:13-24, 1416:4-17.

507. Dr. Striegel explained how the functions related to Cisco's infringing functionality. *See* Tr. 1423:4-22, 1432:9-20; Tr. 1432:21-1433:18; Tr. 1376:17-1378:14 (explaining why routing and switching capabilities play a role in infringement). He "considered whether further apportionment would be necessary" and concluded that further parsing sub-features would "decrease" the integrity of his analysis, which focused on Cisco's representations of the core product functionality. Tr. 1414:13-24.

508. Each top-level function identified in Cisco's Accused Products are weighted equally for the purposes of identifying the footprint of Centripetal's patented technology in Cisco's Accused Products. Tr. 1338:16-1342:17. For example, certain functions "could be different weights for different customers," possibly due to "the particular deployment scenario." *Id.* To provide a firm and more objective foundation for his analysis, Dr. Striegel used Cisco's documents to determine what Cisco conveys to customers as "the key benefits, . . . the features, what should you expect if you were to go out and purchase this product," giving those equal weight. Tr. at 1338:16-1339:24, 1427:24-1429:2.

509. While the infringing top-level functions of Cisco's Accused Products could have reasonably been weighted more heavily, they were weighted equally to be conservative and thereby narrowing the footprint of Centripetal's patented technology in Cisco's Accused Products. Tr. 1340:22-1341:17.

510. PTX-1931 is a summary of the apportionment for each product that was provided in Dr. Striegel's testimony. This chart depicts the total number of top-level functions that Dr. Striegel identified for each category of Accused Product based on Cisco's technical information, and in the far right column identifies the number of those functions that he found to infringe for each Asserted Patent. By dividing the number of infringing functions for each Asserted Patent by the number of total functions, Dr. Striegel identified what percentage of each Accused Product infringed each Asserted Patent. His underlying analysis is discussed in greater detail below.

Accused Products	Total # of Top-Level Functions	# Infringing Top-Level Functions
Catalyst 9000 switches	13	**6** ('856, '205, '193 Patents) **5** ('176 Patent) **4** ('806 Patent)
Integrated Services Routers 1000, 4000	9	**4** (All Patents)
Aggregated Services Routers 1000	8	**2** (All Patents)
Firepower firewall / Adaptive Security Appliance	13	**6** ('205 Patent) **7** ('806 Patent)
Digital Network Architecture	10	**3** ('205, '806 Patents)
Stealthwatch	5	**4** ('176, '856 Patents)
Identity Services Engine	13	**5** ('856 Patent)

PTX-1931.

ii. Apportionment of the Catalyst 9000 Switches

511. The Catalyst 9000 switches have 13 top-level functions when analyzed and categorized by features and commodity components, which are shown on PTX-409 at 847-48 and which is reproduced below. Tr. 1342:25-1348:1; PTX-409 at 847-48.

Product overview

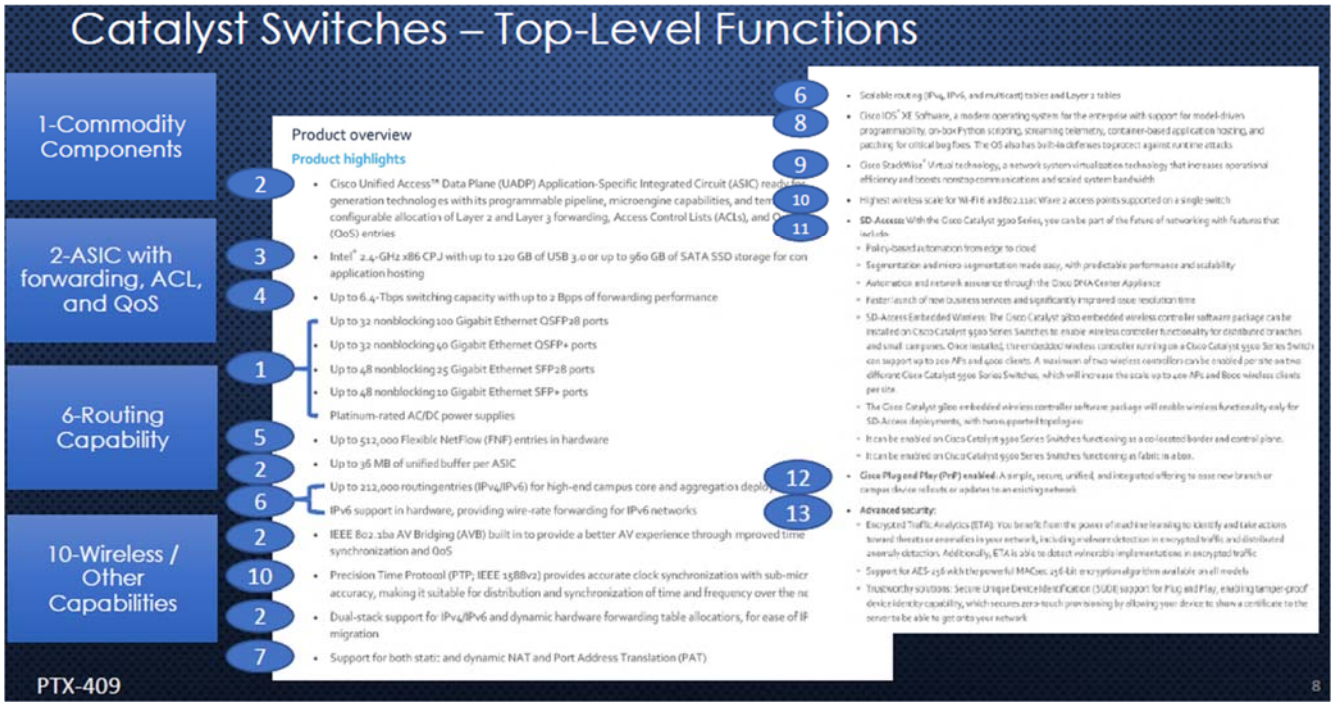
Product highlights

- Cisco Unified Access™ Data Plane (UADP) Application-Specific Integrated Circuit (ASIC) ready for next-generation technologies with its programmable pipeline, microengine capabilities, and template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality-of-Service (QoS) entries
- Intel® 2.4-GHz x86 CPU with up to 120 GB of USB 3.0 or up to 960 GB of SATA SSD storage for container-based application hosting
- Up to 6.4-Tbps switching capacity with up to 2 Bpps of forwarding performance
- Up to 32 nonblocking 100 Gigabit Ethernet QSFP28 ports
- Up to 32 nonblocking 40 Gigabit Ethernet QSFP+ ports
- Up to 48 nonblocking 25 Gigabit Ethernet SFP28 ports
- Up to 48 nonblocking 10 Gigabit Ethernet SFP+ ports
- Platinum-rated AC/DC power supplies
- Up to 512,000 Flexible NetFlow (FNF) entries in hardware
- Up to 36 MB of unified buffer per ASIC
- Up to 212,000 routing entries (IPv4/IPv6) for high-end campus core and aggregation deployments
- IPv6 support in hardware, providing wire-rate forwarding for IPv6 networks
- IEEE 802.1ba AV Bridging (AVB) built in to provide a better AV experience through improved time synchronization and QoS
- Precision Time Protocol (PTP; IEEE 1588v2) provides accurate clock synchronization with sub-microsecond accuracy, making it suitable for distribution and synchronization of time and frequency over the network
- Dual-stack support for IPv4/IPv6 and dynamic hardware forwarding table allocations, for ease of IPv4-to-IPv6 migration
- Support for both static and dynamic NAT and Port Address Translation (PAT)

- Scalable routing (IPv4, IPv6, and multicast) tables and Layer 2 tables
- Cisco IOS® XE Software, a modern operating system for the enterprise with support for model-driven programmability, on-box Python scripting, streaming telemetry, container-based application hosting, and patching for critical bug fixes. The OS also has built-in defenses to protect against runtime attacks
- Cisco StackWise® Virtual technology, a network system virtualization technology that increases operational efficiency and boosts nonstop communications and scaled system bandwidth
- Highest wireless scale for Wi-Fi 6 and 802.11ac Wave 2 access points supported on a single switch
- **SD-Access:** With the Cisco Catalyst 9500 Series, you can be part of the future of networking with features that include:
  - Policy-based automation from edge to cloud
  - Segmentation and micro-segmentation made easy, with predictable performance and scalability
  - Automation and network assurance through the Cisco DNA Center Appliance
  - Faster launch of new business services and significantly improved issue resolution time
  - SD-Access Embedded Wireless: The Cisco Catalyst 9800 embedded wireless controller software package can be installed on Cisco Catalyst 9500 Series Switches to enable wireless controller functionality for distributed branches and small campuses. Once installed, the embedded wireless controller running on a Cisco Catalyst 9500 Series Switch can support up to 200 APs and 4000 clients. A maximum of two wireless controllers can be enabled per site on two different Cisco Catalyst 9500 Series Switches, which will increase the scale up to 400 APs and 8000 wireless clients per site.
  - The Cisco Catalyst 9800 embedded wireless controller software package will enable wireless functionality only for SD-Access deployments, with two supported topologies:
  - It can be enabled on Cisco Catalyst 9500 Series Switches functioning as a co-located border and control plane.
  - It can be enabled on Cisco Catalyst 9500 Series Switches functioning as fabric in a box.
- **Cisco Plug and Play (PnP) enabled**: A simple, secure, unified, and integrated offering to ease new branch or campus device rollouts or updates to an existing network
- **Advanced security:**
  - Encrypted Traffic Analytics (ETA): You benefit from the power of machine learning to identify and take actions toward threats or anomalies in your network, including malware detection in encrypted traffic and distributed anomaly detection. Additionally, ETA is able to detect vulnerable implementations in encrypted traffic
  - Support for AES-256 with the powerful MACsec 256-bit encryption algorithm available on all models
  - Trustworthy solutions: Secure Unique Device Identification (SUDI) support for Plug and Play, enabling tamper-proof device identity capability, which secures zero-touch provisioning by allowing your device to show a certificate to the server to be able to get onto your network

PTX-409 at 847-48.

512. The demonstrative below which was shown during the direct examination of Dr. Striegel, shows the grouping of top-level functions. Tr. 1344:20-1354:22.



513. Group 1 covers the commodity components for the Catalyst 9000 Switches, which are the physical configuration of the hardware, including the number of ports and different power supplies. These commodity components are grouped because they are "reasonably standardized" industry components that are not "particularly distinctive" outside of possibly being adapted to a particular configuration. Tr. 1344:11-1345:22.

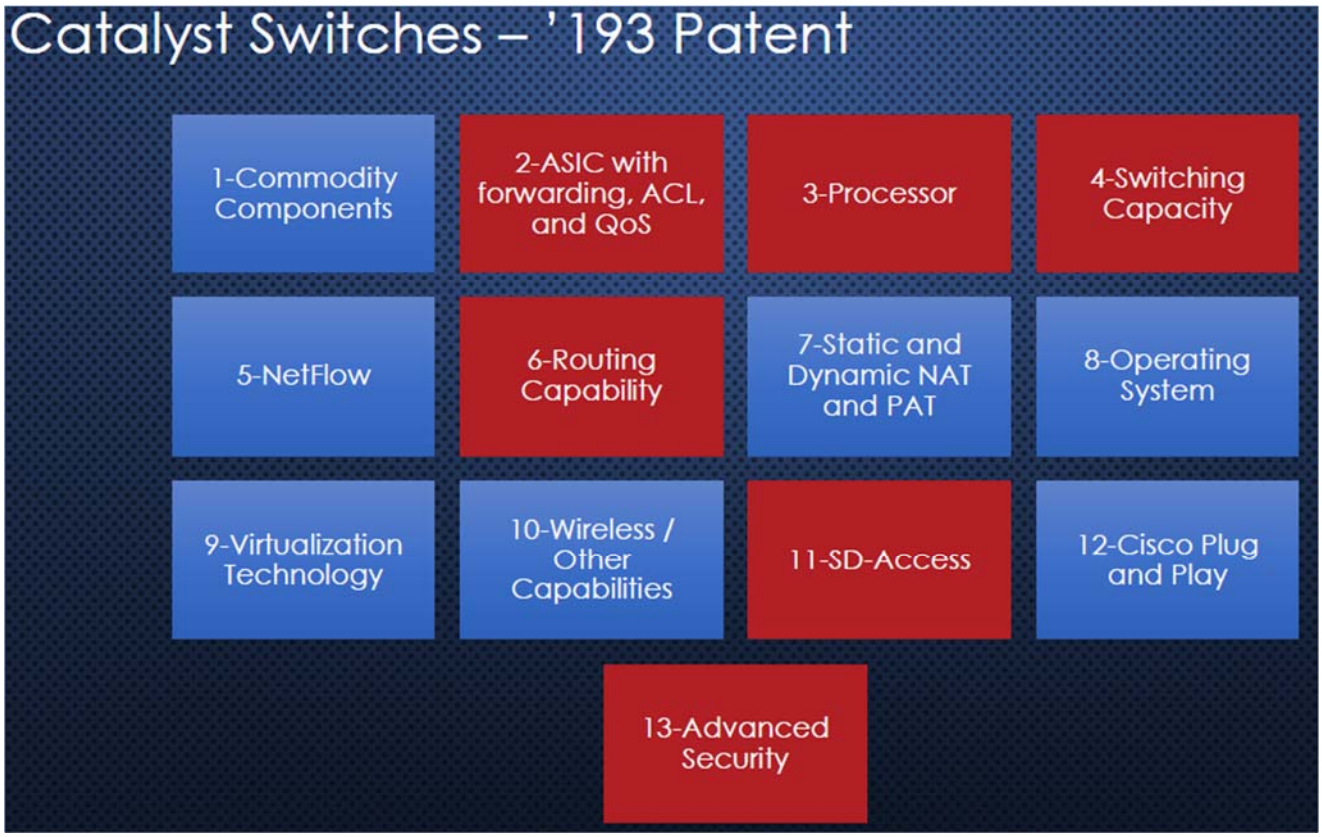
514. Group 2 covers the Unified Access Data Plane ("UADP"), which includes the Application-Specific Integrated Circuit ("ASIC"), Access Control Lists ("ACL"), Quality of Services (QoS) and AV Bridging, and forwarding table allocations. Tr. 1345:23-1346:15.

515. Group 6 covers the routing function. Tr. 1346:16-21.

516. Group 10 groups the wireless and related capabilities. Tr. 1346:22-1347:3.

517. The remaining features identified by Cisco in PTX-409 at 847-48 were mapped directly to high-level functions as Cisco identified them. Tr. 1347:4-6.

518. Of the 13 top-level functions of the Cisco Catalyst 9000 switches, six are covered by the '193 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1348:14-1350:2.



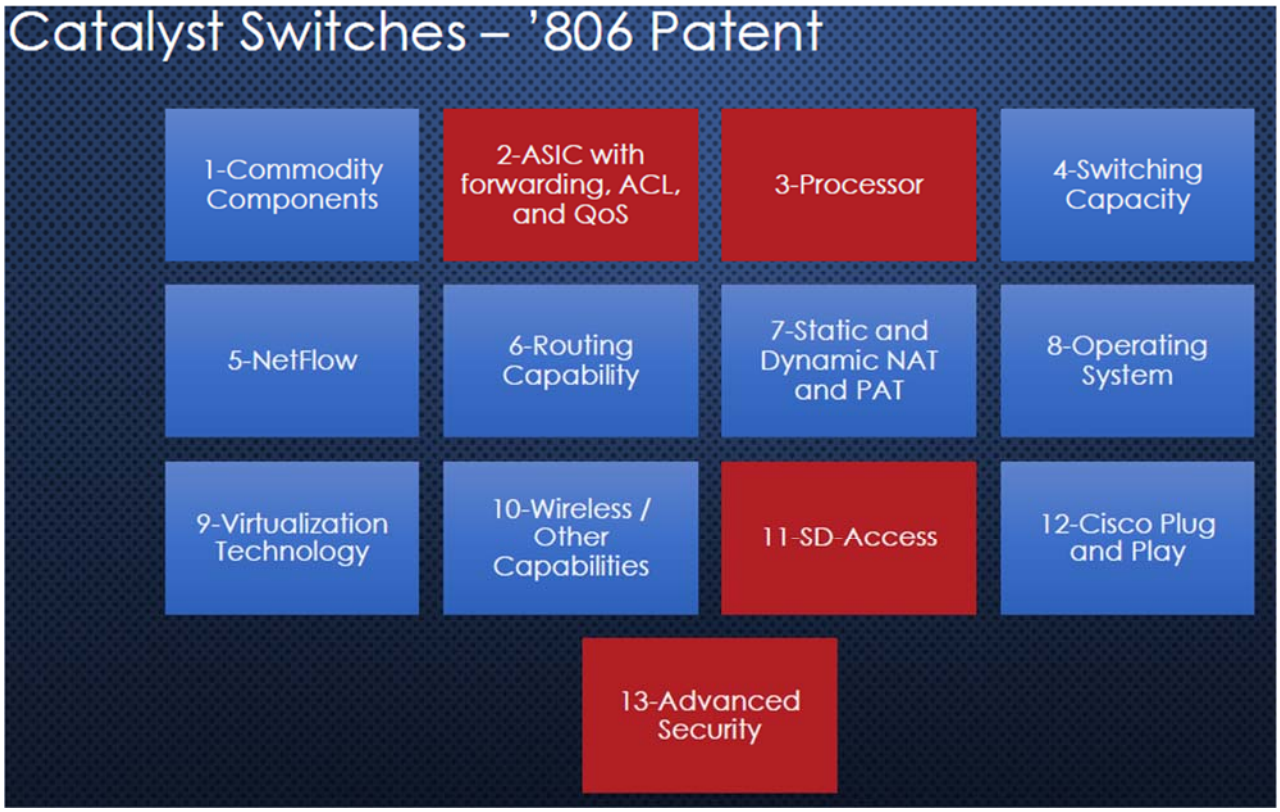
519. The '193 Patent covers ASIC, Processor, and Switching because they are directly identified in the claims. Tr. 1348:17-24.

520. The '193 Patent covers routing because it relates to the forwarding and dropping packets on the routing. Tr. 1348:24-1349:1.

521. The '193 Patent covers SD-Access because it relates to the pushing of rules to the particular switch. Tr. 1349:1-2.

522. The '193 Patent covers Advanced Security because it relates to the network security aspects of the device. Tr. 1349:2-4.

523. Of the 13 top-level functions of the Cisco Catalyst 9000 switches, four are covered by the '806 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1352:25-1352:7.



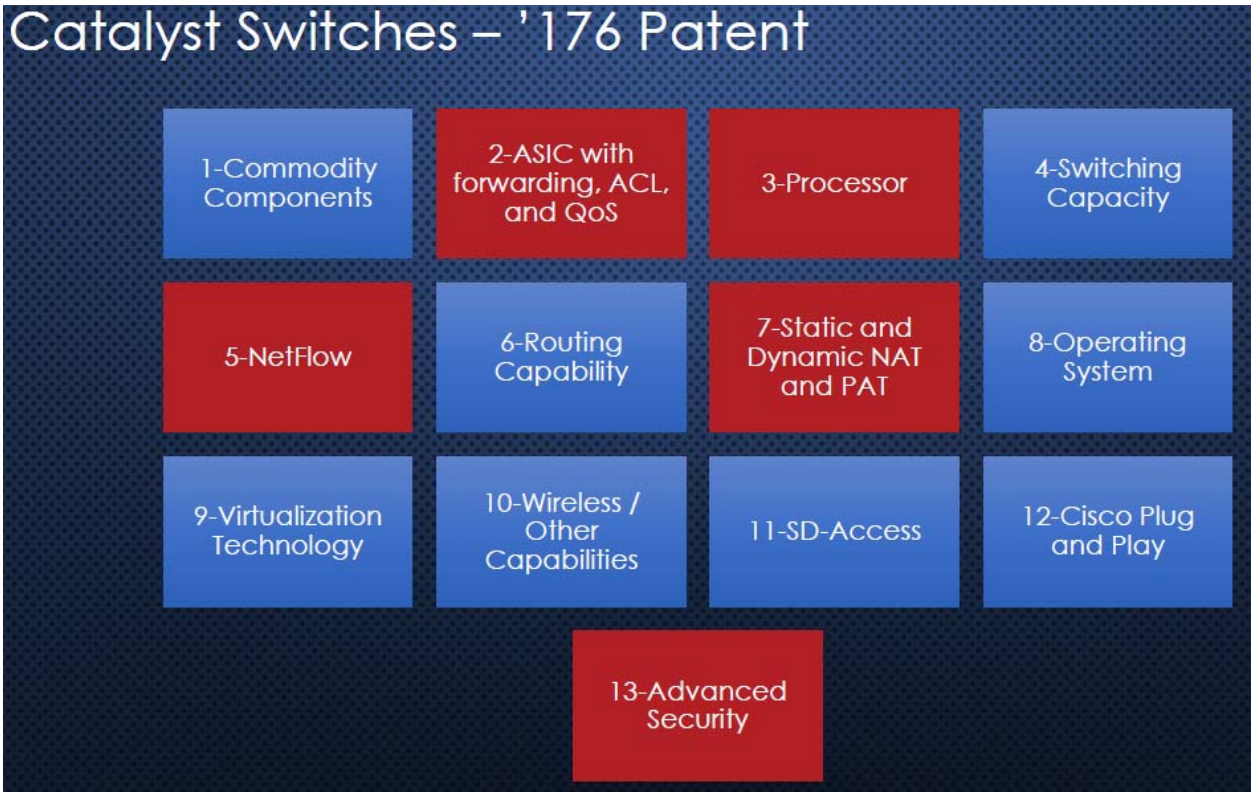
524. The '806 Patent covers ASIC because it is directly identified in the claims by virtue of using the rule set. Tr. 1353:2-4.

525. The '806 Patent covers Processor because it relates to preprocessing or rules. Tr. 1353:4-5.

526. The '806 Patent covers SD-Access because it relates to the switching of rules. Tr. 1353:5.

527. The '806 Patent covers Advanced Security because it relates to the network security aspects of the device. Tr. 1353:6-7.

528. Of the 13 top-level functions of the Cisco Catalyst 9000 switches, five are covered by the '176 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1354:3-13.



529. The '176 Patent covers ASIC and Processor because they are directly identified in the claims. Tr. 1354:6-8.

530. The '176 Patent covers Netflow because it relates to the Netflow being correlated based on log entries. Tr. 1354:8-9.

531. The '176 Patent relates to Static and Dynamic NAT and PAT because of its use in correlating log entries. Tr. 1354:9-11.

532. The '176 Patent relates to Advanced Security because of the security aspect. Tr. 1354:12-13.

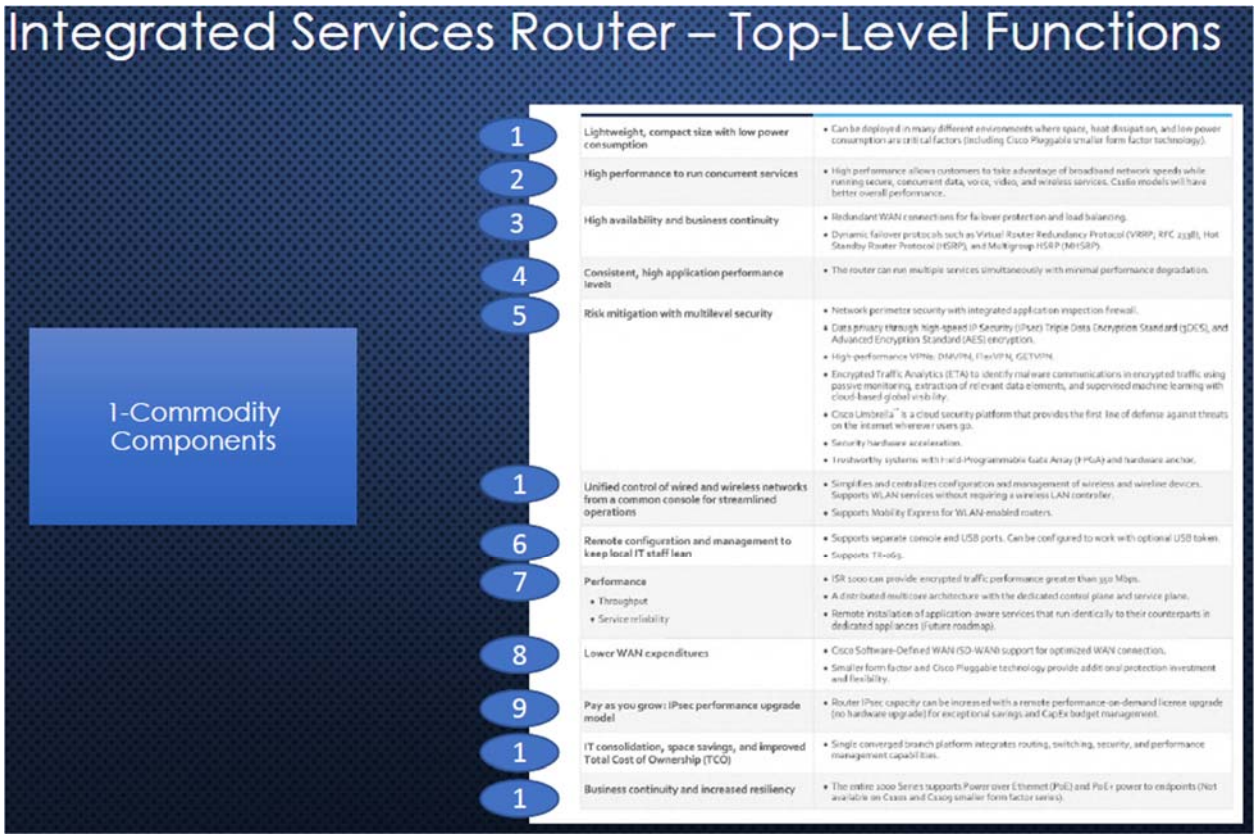
iii. Apportionment of the ISR Routers

533. The Integrated Services Routers (ISR) 1000 and 4000 have nine top-level functions when standardized by features and commodity components, which are shown on PTX-412 at 899 and which is reproduced below. Tr. 1355:12-24; PTX-412 at 899.

Business need	Features/description
Lightweight, compact size with low power consumption	• Can be deployed in many different environments where space, heat dissipation, and low power consumption are critical factors (including Cisco Pluggable smaller form factor technology).
High performance to run concurrent services	• High performance allows customers to take advantage of broadband network speeds while running secure, concurrent data, voice, video, and wireless services. C1160 models will have better overall performance.
High availability and business continuity	• Redundant WAN connections for failover protection and load balancing. • Dynamic failover protocols such as Virtual Router Redundancy Protocol (VRRP; RFC 2338), Hot Standby Router Protocol (HSRP), and Multigroup HSRP (MHSRP).
Consistent, high application performance levels	• The router can run multiple services simultaneously with minimal performance degradation.
Risk mitigation with multilevel security	• Network perimeter security with integrated application inspection firewall. • Data privacy through high-speed IP Security (IPsec) Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) encryption. • High-performance VPNs: DMVPN, FlexVPN, GETVPN. • Encrypted Traffic Analytics (ETA) to identify malware communications in encrypted traffic using passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. • Cisco Umbrella™ is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. • Security hardware acceleration. • Trustworthy systems with Field-Programmable Gate Array (FPGA) and hardware anchor.
Unified control of wired and wireless networks from a common console for streamlined operations	• Simplifies and centralizes configuration and management of wireless and wireline devices. Supports WLAN services without requiring a wireless LAN controller. • Supports Mobility Express for WLAN-enabled routers.
Remote configuration and management to keep local IT staff lean	• Supports separate console and USB ports. Can be configured to work with optional USB token. • Supports TR-069.
Performance • Throughput • Service reliability	• ISR 1000 can provide encrypted traffic performance greater than 350 Mbps. • A distributed multicore architecture with the dedicated control plane and service plane. • Remote installation of application-aware services that run identically to their counterparts in dedicated appliances (Future roadmap).
Lower WAN expenditures	• Cisco Software-Defined WAN (SD-WAN) support for optimized WAN connection. • Smaller form factor and Cisco Pluggable technology provide additional protection investment and flexibility.
Pay as you grow: IPsec performance upgrade model	• Router IPsec capacity can be increased with a remote performance-on-demand license upgrade (no hardware upgrade) for exceptional savings and CapEx budget management.
IT consolidation, space savings, and improved Total Cost of Ownership (TCO)	• Single converged branch platform integrates routing, switching, security, and performance management capabilities.
Business continuity and increased resiliency	• The entire 1000 Series supports Power over Ethernet (PoE) and PoE+ power to endpoints (Not available on C1101 and C1109 smaller form factor series).

PTX-412 at 899.

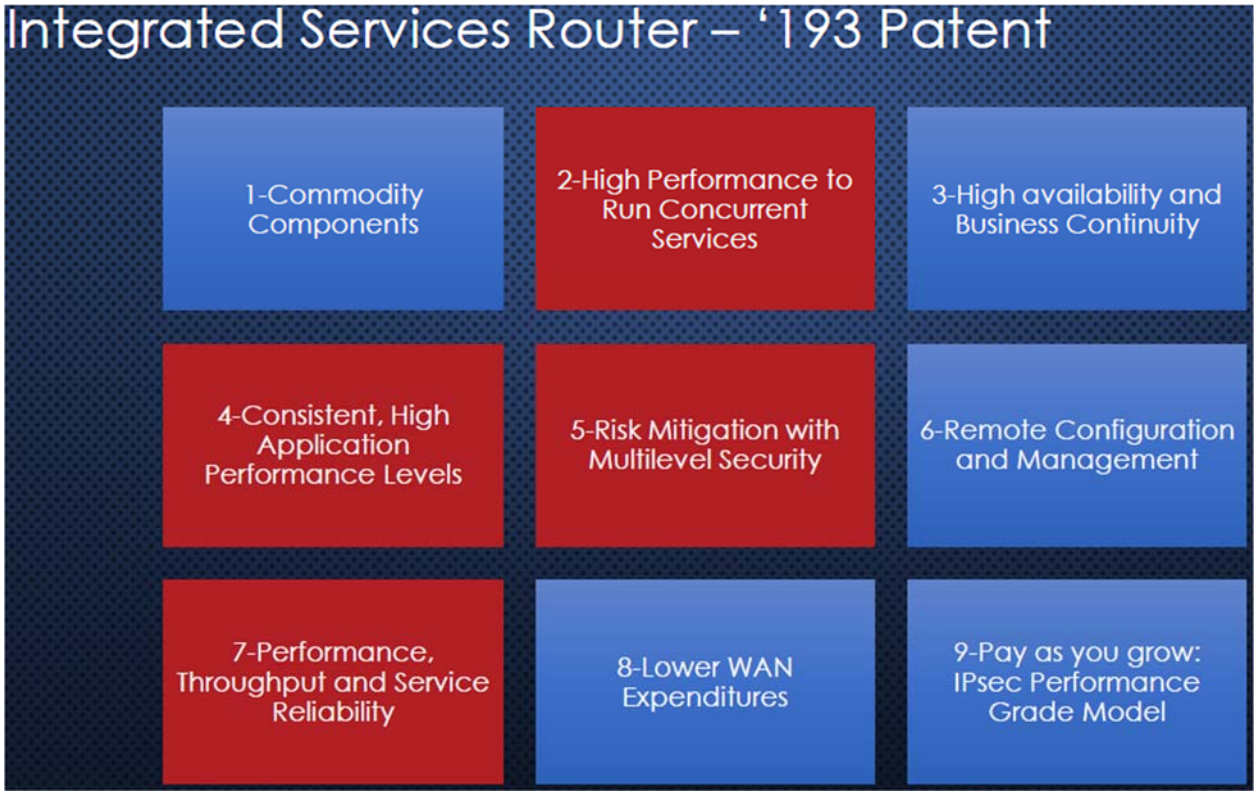
534. The demonstrative below which was shown during the direct examination of Dr. Striegel, shows the grouping of top-level functions. Tr. 1355:5-24.



535. Group 1 covers the commodity components for the ISR Routers, which are grouped because they are hardware components that are common across the industry and general commodity components that are typical in this type of product. Tr. 1355:20-24.

536. The remaining features identified by Cisco in PTX-409 at 847-48 map directly to high-level functions as Cisco identified them. Tr. 1354:23-1355:24.

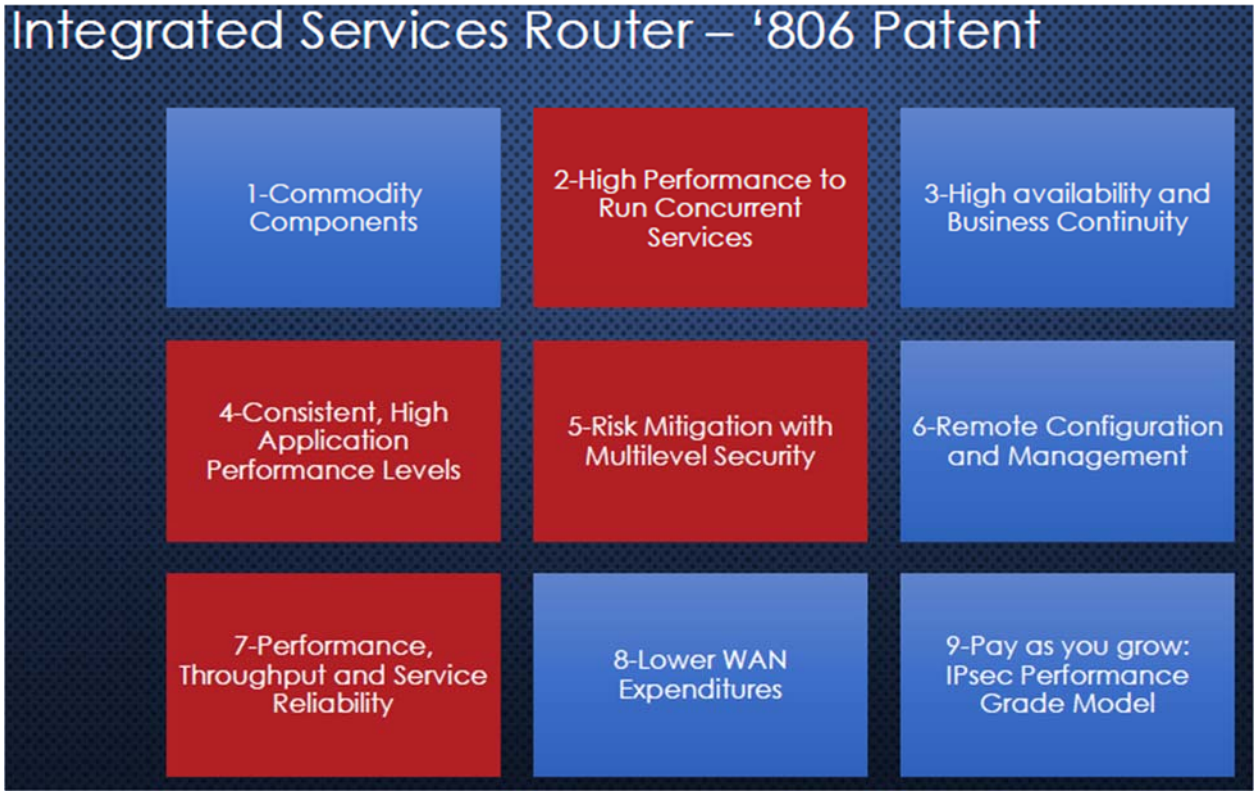
537. Of the nine top-level functions of the ISR Routers, four are covered by the '193 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1355:25-1356:10.



538. The '193 Patent relates to High Performance to Run Concurrent Services, Consistent, High Application Performance Levels, and Performance, Throughput and Service Reliability because of the processor in the claims. Tr. 1355:25-1356-10.

539. The '193 Patent relates to Risk Mitigation with Multilevel Security because of the network security offered by the '193 Patent. Tr. 1355:25-1356:10.

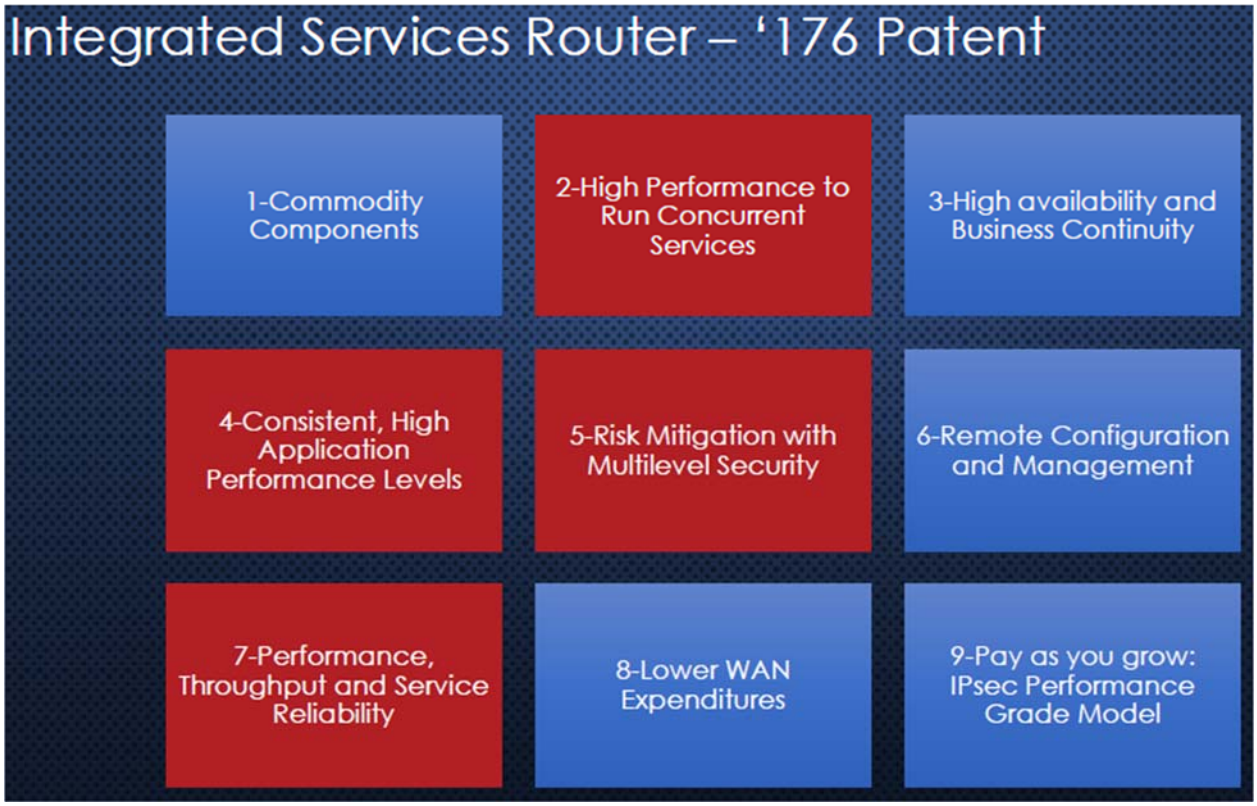
540. Of the nine top-level functions of the ISR Routers, four are covered by the '806 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1356:11-19.



541. The '806 Patent relates to High Performance to Run Concurrent Services, Consistent, High Application Performance Levels, and Performance, Throughput and Service Reliability because of the processor in the claims. Tr. 1355:25-1356:19.

542. The '806 Patent relates to Risk Mitigation with Multilevel Security because of the network security offered by the '806 Patent. Tr. 1355:25-1356:19.

543. Of the nine top-level functions of the ISR Routers, four are covered by the '176 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1357:21-1358:3.



544. The '176 Patent relates to High Performance to Run Concurrent Services, Consistent, High Application Performance Levels, and Performance, Throughput and Service Reliability because the processor in the '176 Patent is necessary for these high-performance attributes. Tr. 1357:21-1358:3.

545. The '176 Patent relates to Risk Mitigation with Multilevel Security because of the network security offered by the '176 Patent. Tr. 1357:21-1358:3.

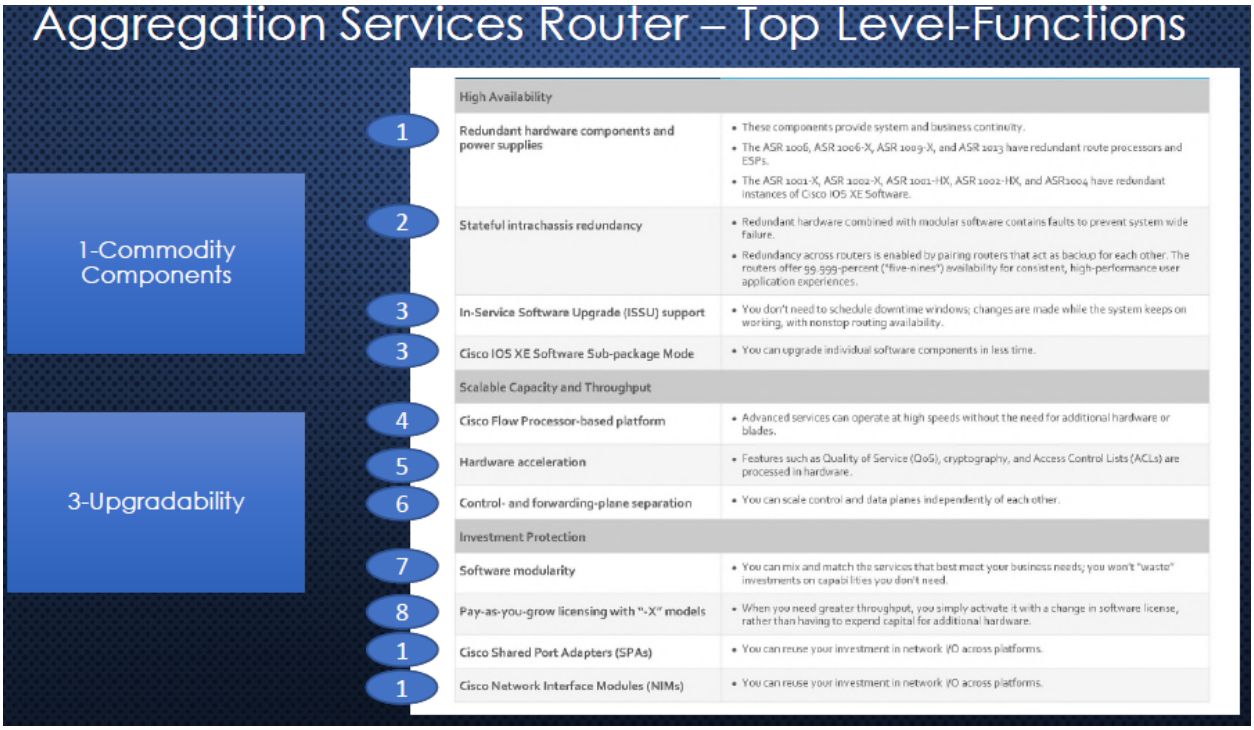
iv. Apportionment of the ASR Routers

546. The Aggregated Services Routers (ASR) 1000 and 4000 have nine top-level functions when standardized by features and commodity components, which are shown on PTX-575 at 936 and which is reproduced below. Tr. 1358:11-1359:21; PTX-575 at 936.

Feature	Benefit
High Availability	
Redundant hardware components and power supplies	• These components provide system and business continuity. • The ASR 1006, ASR 1006-X, ASR 1009-X, and ASR 1013 have redundant route processors and ESPs. • The ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, and ASR1004 have redundant instances of Cisco IOS XE Software.
Stateful intrachassis redundancy	• Redundant hardware combined with modular software contains faults to prevent system wide failure. • Redundancy across routers is enabled by pairing routers that act as backup for each other. The routers offer 99.999-percent ("five-nines") availability for consistent, high-performance user application experiences.
In-Service Software Upgrade (ISSU) support	• You don't need to schedule downtime windows; changes are made while the system keeps on working, with nonstop routing availability.
Cisco IOS XE Software Sub-package Mode	• You can upgrade individual software components in less time.
Scalable Capacity and Throughput	
Cisco Flow Processor-based platform	• Advanced services can operate at high speeds without the need for additional hardware or blades.
Hardware acceleration	• Features such as Quality of Service (QoS), cryptography, and Access Control Lists (ACLs) are processed in hardware.
Control- and forwarding-plane separation	• You can scale control and data planes independently of each other.
Investment Protection	
Software modularity	• You can mix and match the services that best meet your business needs; you won't "waste" investments on capabilities you don't need.
Pay-as-you-grow licensing with "-X" models	• When you need greater throughput, you simply activate it with a change in software license, rather than having to expend capital for additional hardware.
Cisco Shared Port Adapters (SPAs)	• You can reuse your investment in network I/O across platforms.
Cisco Network Interface Modules (NIMs)	• You can reuse your investment in network I/O across platforms.

PTX-575 at 936.

547. The demonstrative below which was shown during the direct examination of Dr. Striegel, shows the grouping of top-level functions. Tr. 1359:7-21.

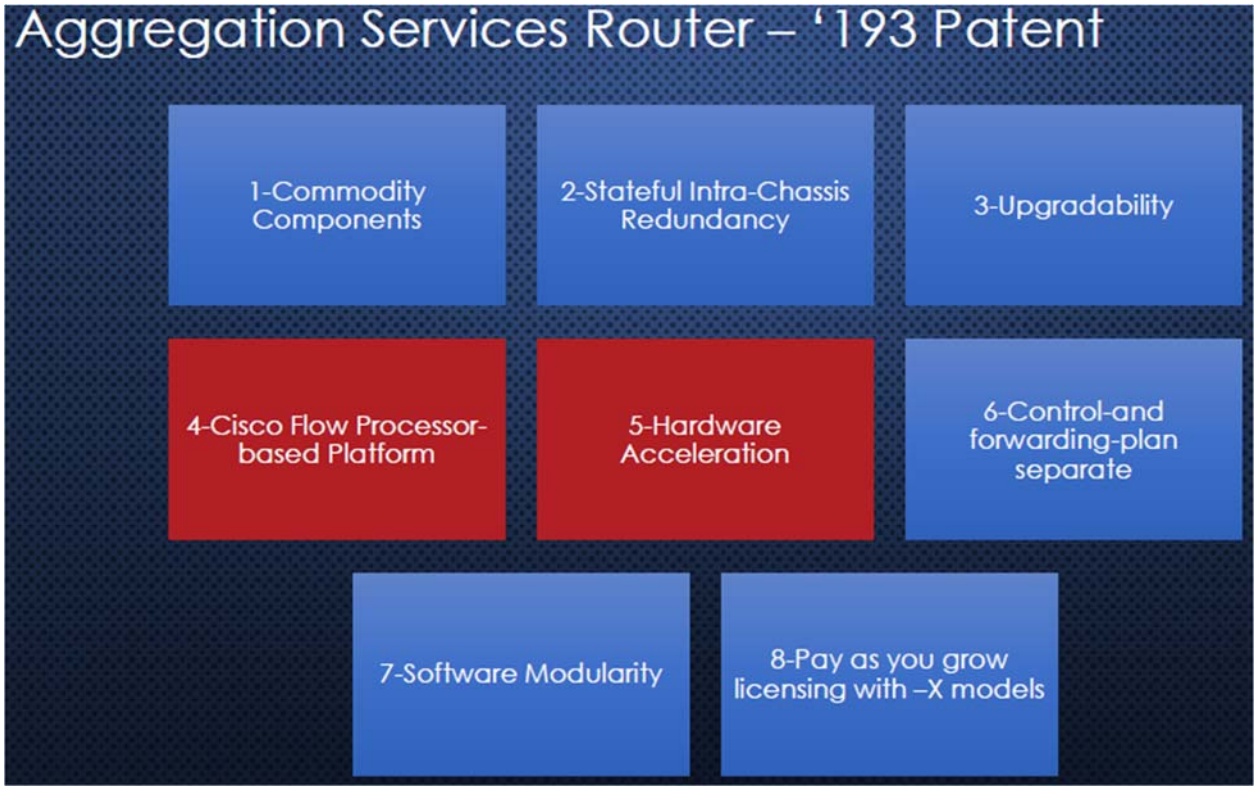


548. Group 1 covers the commodity components for the ASR Routers, which are grouped because they are hardware components that are common across the industry and general commodity components that are typical in this type of product. Tr. 1359:13-16.

549. Group 3 covers upgradeability for the ASR Routers. Tr. 1359:13-16.

550. The remaining features identified by Cisco in PTX-575 at 936 map directly to high-level functions as Cisco identified them. Tr. 1358:11-1359:21.

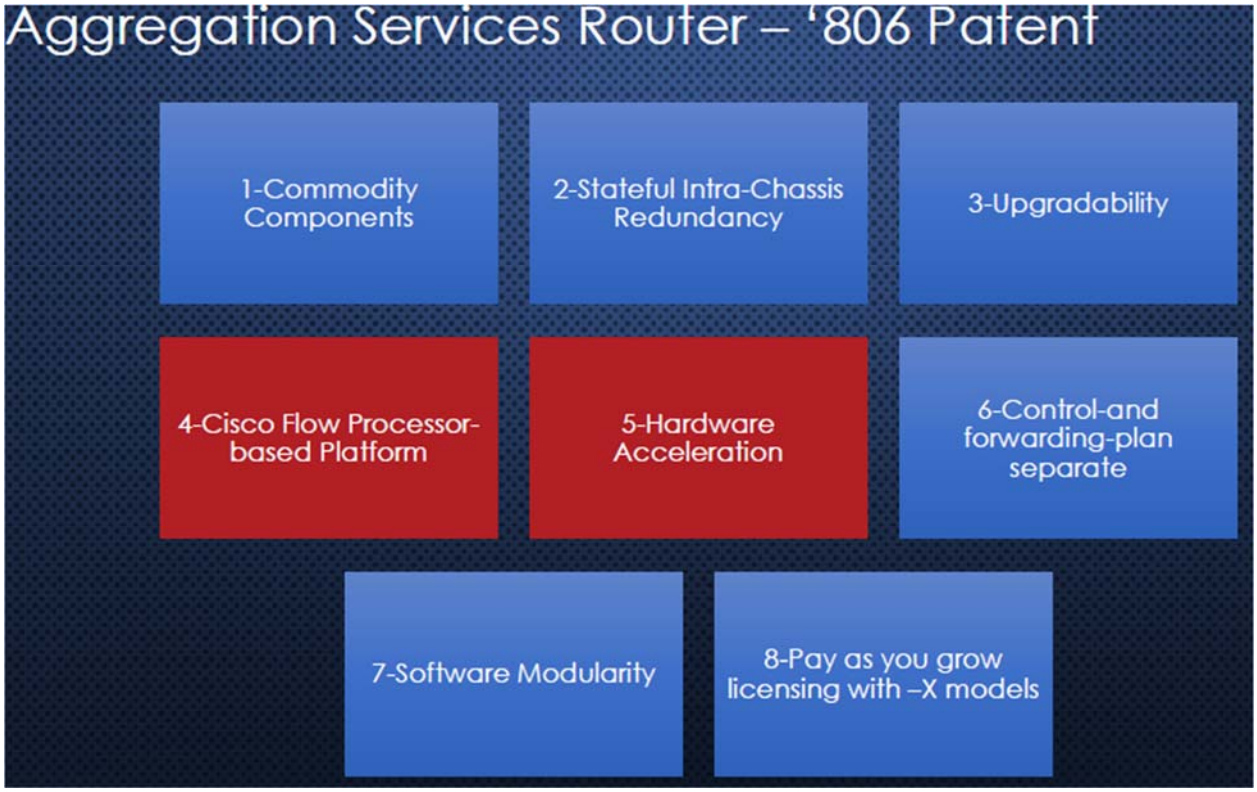
551. Of the eight top-level functions of the ASR Routers, two are covered by the '193 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1359:22-1360:4.



552. The '193 Patent relates to Flow Processor-based Platform because the flow processor is directly in the claims for forwarding traffic. Tr. 1359:22-1360:2.

553. The '193 Patent relates to Hardware Acceleration because of the security capability offered by the '193 Patent. Tr. 1359:22-1360:4.

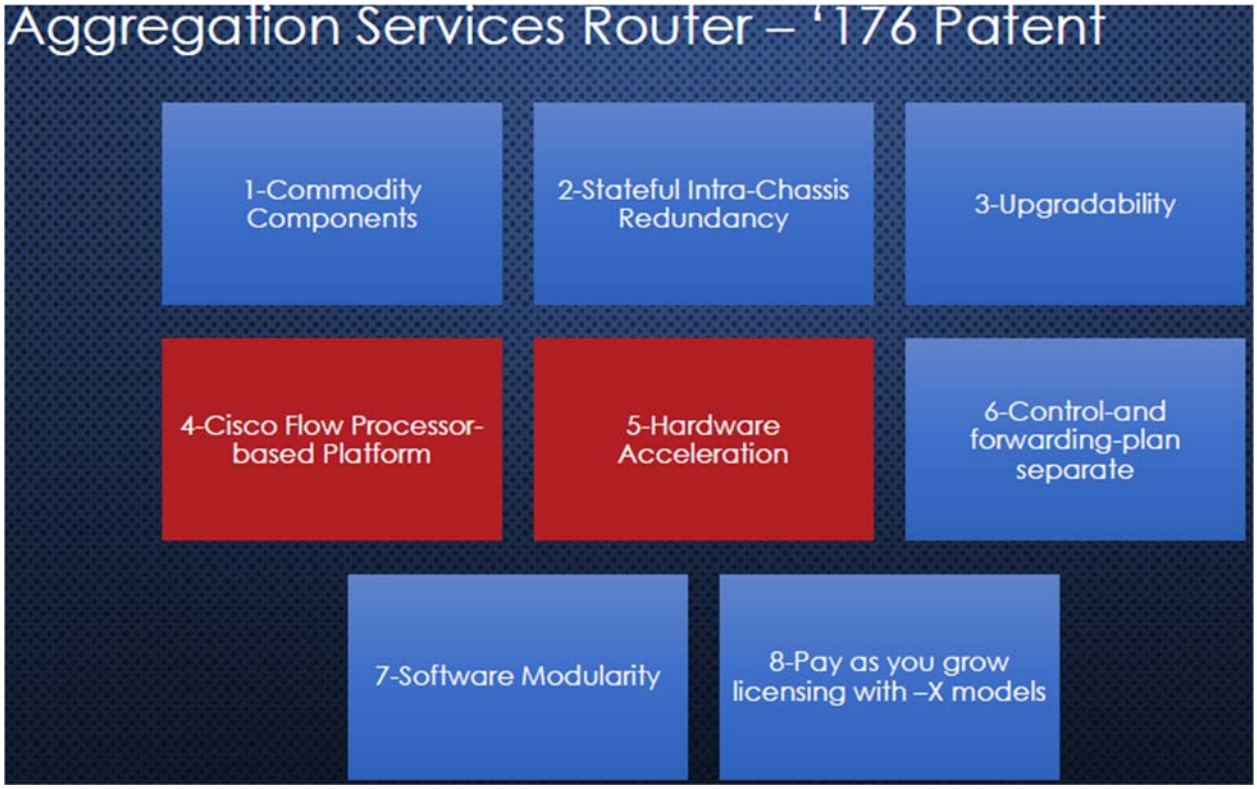
554. Of the eight top-level functions of the ASR Routers, two are covered by the '193 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1360:5-11.



555. The '806 Patent relates to Flow Processor-based Platform because the usage of rules flow processor is directly in the claims for forwarding traffic. Tr. 1360:5-11.

556. The '806 Patent relates to Hardware Acceleration because of the usage of rules offered by the '806 Patent. Tr. 1360:5-11.

557. Of the eight top-level functions of the ASR Routers, two are covered by the '193 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1361:6-13.



558. The '176 Patent relates to Flow Processor-based Platform because it is directly in the claims due to the packets and rules. Tr. 1361:6-11.

559. The '176 Patent relates to Hardware Acceleration because of the security properties provided by the '176 Patent. Tr. 1360:5-13.

v. Apportionment of the Firewalls

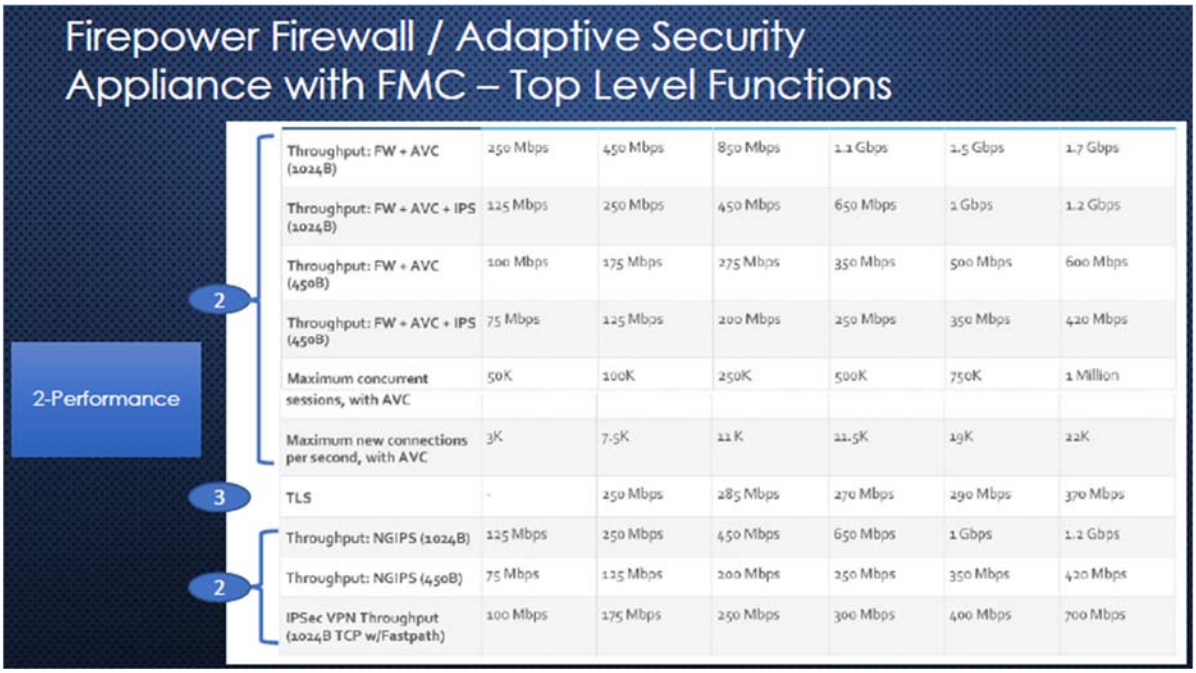
560. The Firewalls have nine top-level functions when standardized by features and commodity components, which are shown on PTX-1106 at 16-18 and which is reproduced below. Tr. 1361:14-1363:13.

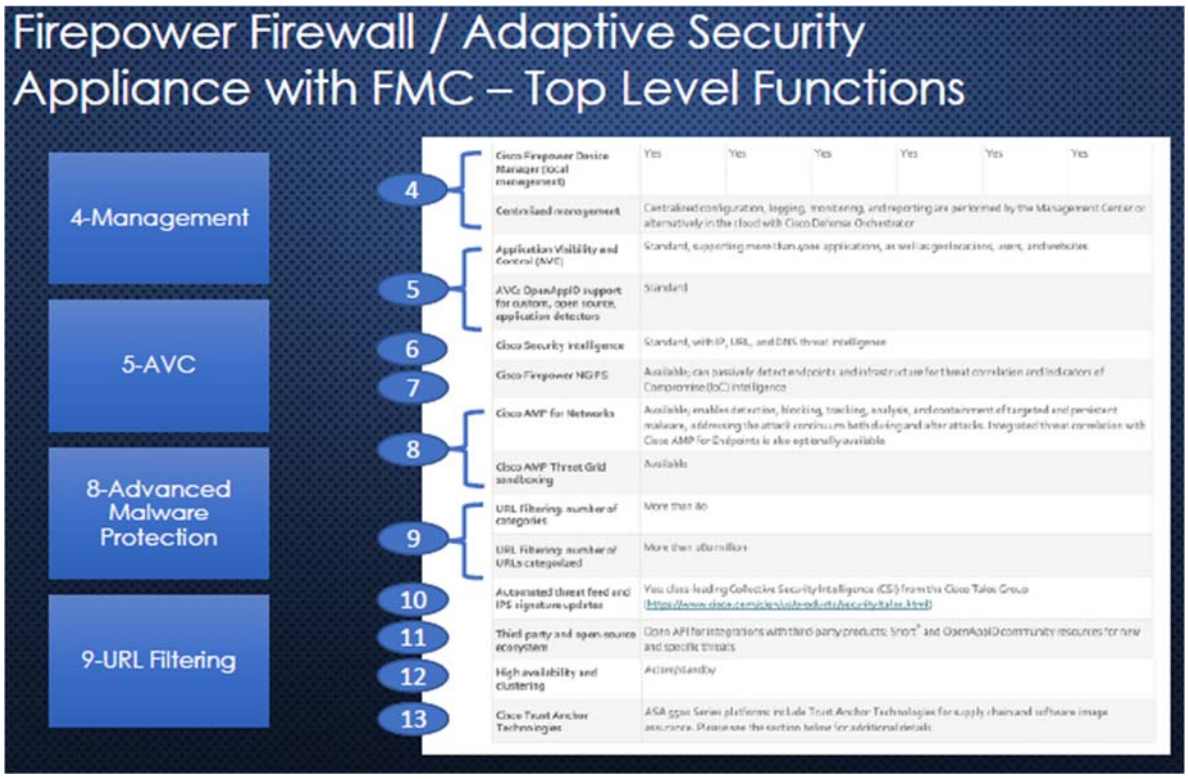
Features	5506	5508	5516	5525	5545	5555
Throughput: FW + AVC (1024B)	250 Mbps	450 Mbps	850 Mbps	1.1 Gbps	1.5 Gbps	1.7 Gbps
Throughput: FW + AVC + IPS (1024B)	125 Mbps	250 Mbps	450 Mbps	650 Mbps	1 Gbps	1.2 Gbps
Throughput: FW + AVC (450B)	100 Mbps	175 Mbps	275 Mbps	350 Mbps	500 Mbps	600 Mbps
Throughput: FW + AVC + IPS (450B)	75 Mbps	125 Mbps	200 Mbps	250 Mbps	350 Mbps	420 Mbps
Maximum concurrent sessions, with AVC	50K	100K	250K	500K	750K	1 Million
Maximum new connections per second, with AVC	3K	7.5K	11 K	11.5K	19K	22K
TLS	-	250 Mbps	285 Mbps	270 Mbps	290 Mbps	370 Mbps
Throughput: NGIPS (1024B)	125 Mbps	250 Mbps	450 Mbps	650 Mbps	1 Gbps	1.2 Gbps
Throughput: NGIPS (450B)	75 Mbps	125 Mbps	200 Mbps	250 Mbps	350 Mbps	420 Mbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	100 Mbps	175 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps

Cisco Firepower Device Manager (local management)	Yes	Yes	Yes	Yes	Yes	Yes
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator					
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites					
AVC: OpenAppID support for custom, open source, application detectors	Standard					
Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence					
Cisco Firepower NGIPS	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence					
Cisco AMP for Networks	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco AMP for Endpoints is also optionally available					
Cisco AMP Threat Grid sandboxing	Available					
URL Filtering: number of categories	More than 80					
URL Filtering: number of URLs categorized	More than 280 million					
Automated threat feed and IPS signature updates	Yes: class-leading Collective Security Intelligence (CSI) from the Cisco Talos Group (https://www.cisco.com/c/en/us/products/security/talos.html)					
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats					
High availability and clustering	Active/standby					
Cisco Trust Anchor Technologies	ASA 5500 Series platforms include Trust Anchor Technologies for supply chain and software image assurance. Please see the section below for additional details					

PTX-1106 at 16-18.

561. The demonstratives below, which were shown during the direct examination of Dr. Striegel, shows the grouping of top-level functions. Tr. 1363:14-1364:25.





562. Group 2 covers different performance aspects of the Firewalls. Tr. 1363:19-1364:8.

563. Group 4 covers different management aspects. Tr. 1364:9-25.

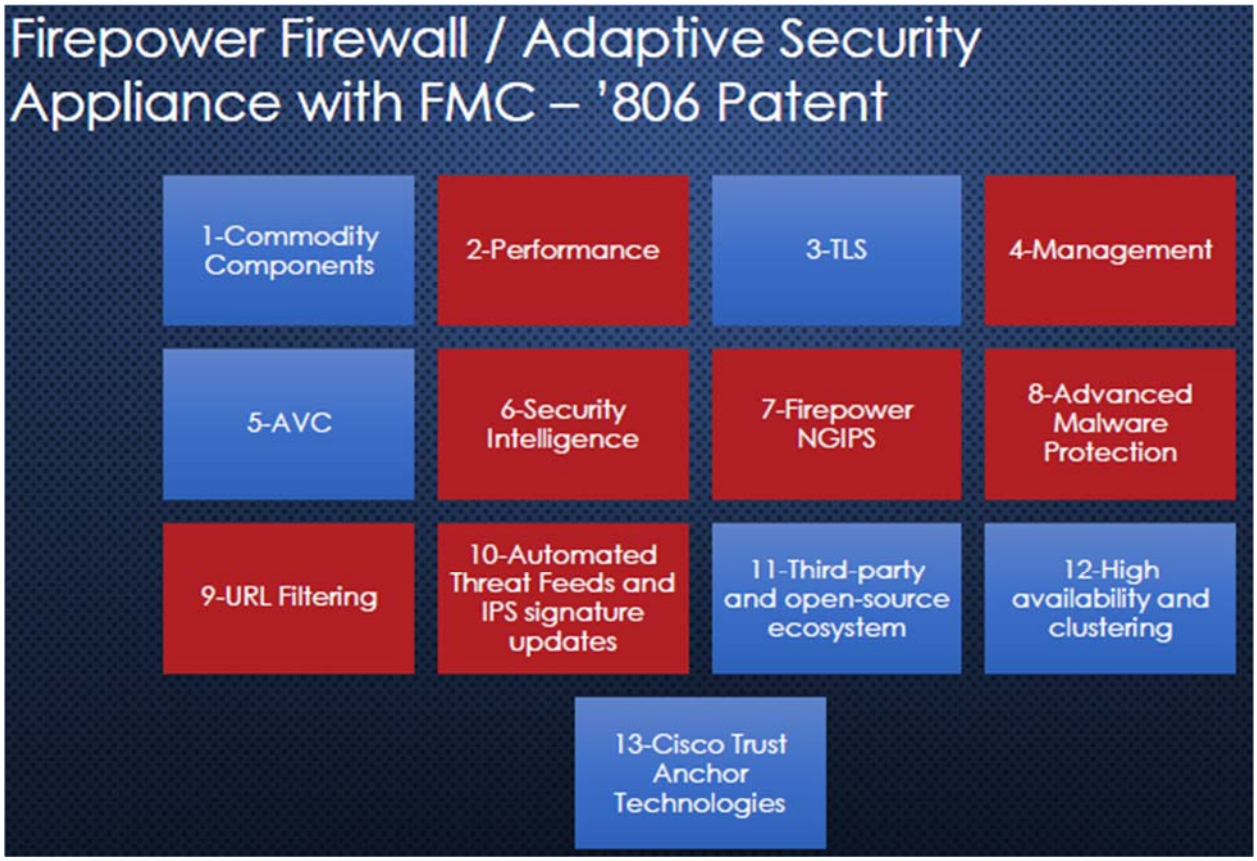
564. Group 5 covers AVC technologies because they are identifying the same capabilities. Tr. 1364:9-25.

565. Group 8 covers AMP technologies because they are identifying the same capabilities. Tr. 1364:9-25.

566. Group 9 covers URL technologies because they are identifying the same capabilities. Tr. 1364:9-25.

567. The remaining features identified by Cisco in PTX-1106 at 040016-18 map directly to high-level functions as Cisco identified them. Tr. 1364:9-25.

568. Of the thirteen top-level functions of the Firewalls, seven are covered by the '806 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1365:1-25.



569. The ’806 Patent relates to Performance because the usage processors with forwarding traffic. Tr. 1365:1-8.

570. The ’806 Patent relates to Management because of the use of security policy managers for packet security gateways. Tr. 1365:1-11.

571. The ’806 Patent relates to the Security Intelligence, Firepower NGIPs, Advanced Malware Protection, URL Filtering, and Automate Threat Feeds and IPS signature updates because of their connection to the network security provided by the ’806 Patent. Tr. 1365:1-17.

vi. Apportionment of DNA

572. DNA has 10 top-level functions when standardized by features and commodity components, which are shown on PTX-410 at 885-86 and which is reproduced below. Tr. 1367:4-1368:1; PTX-419 at 885-86.

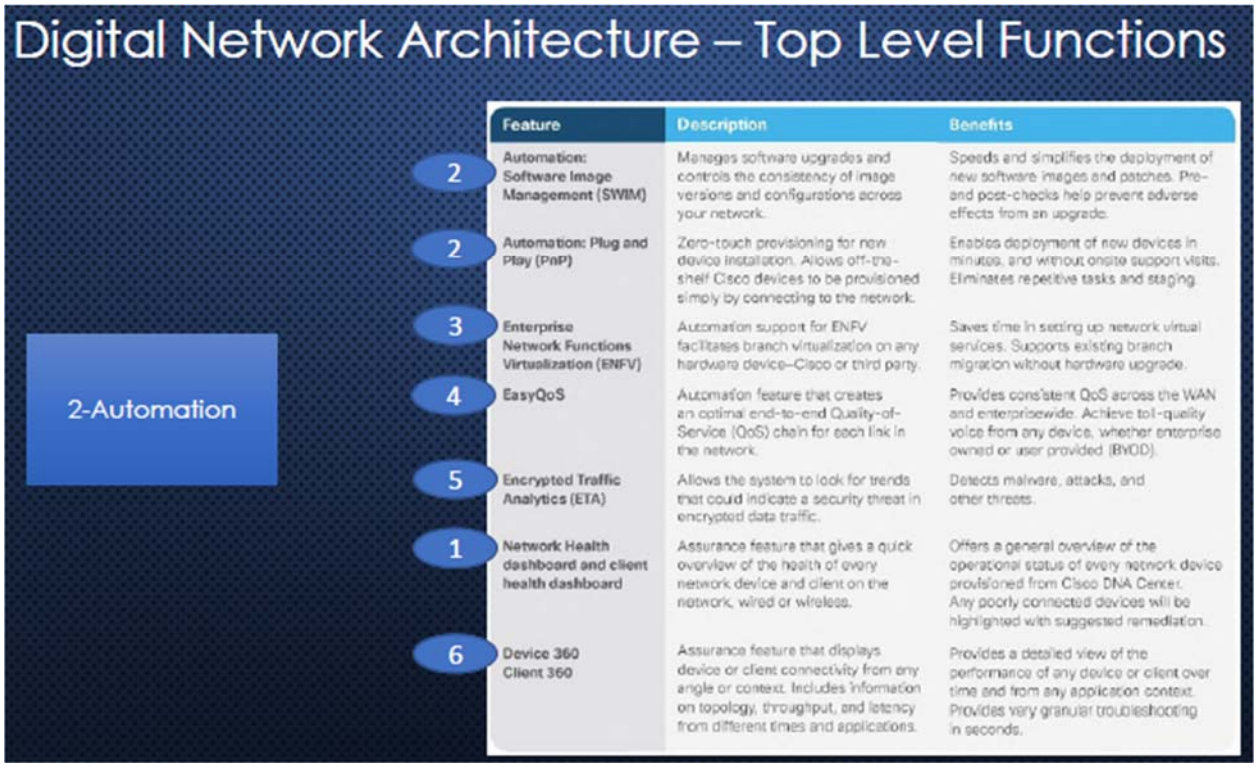
Table 1. Cisco DNA Center features

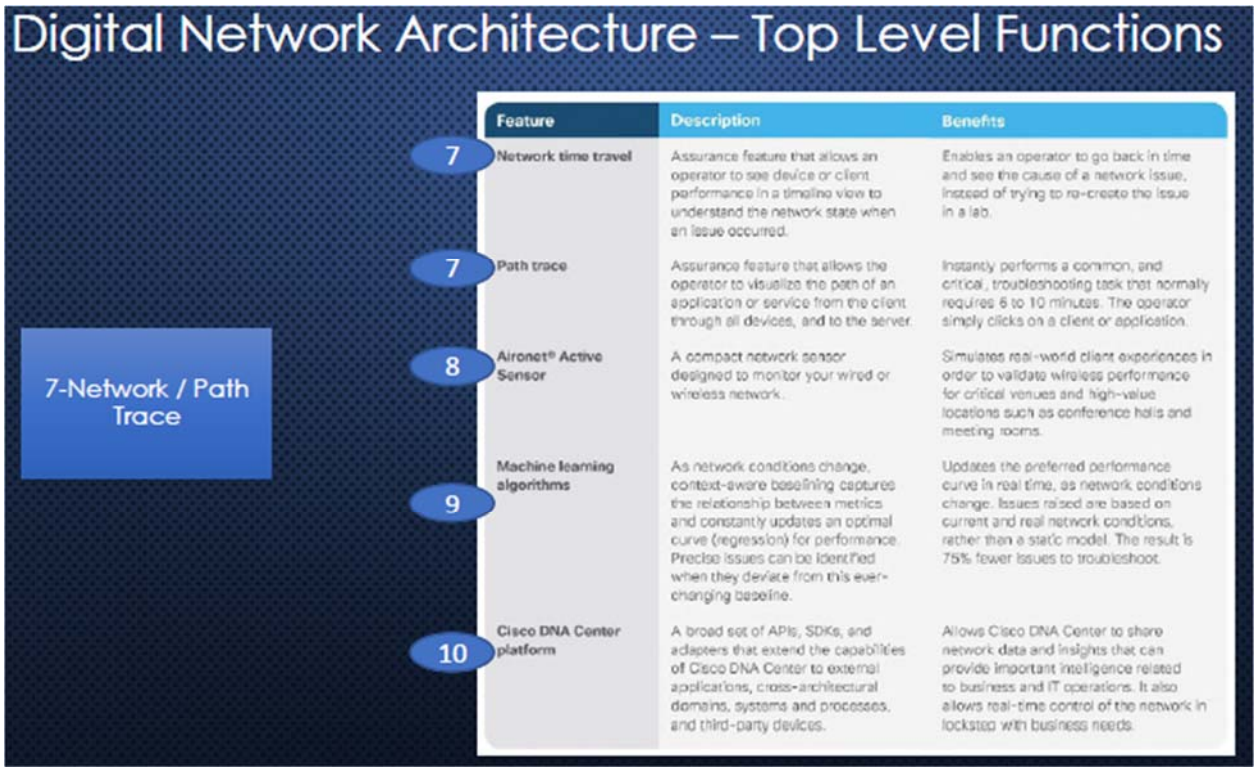
Feature	Description	Benefits
Automation: Software Image Management (SWIM)	Manages software upgrades and controls the consistency of image versions and configurations across your network.	Speeds and simplifies the deployment of new software images and patches. Pre- and post-checks help prevent adverse effects from an upgrade.
Automation: Plug and Play (PnP)	Zero-touch provisioning for new device installation. Allows off-the-shelf Cisco devices to be provisioned simply by connecting to the network.	Enables deployment of new devices in minutes, and without onsite support visits. Eliminates repetitive tasks and staging.
Enterprise Network Functions Virtualization (ENFV)	Automation support for ENFV facilitates branch virtualization on any hardware device—Cisco or third party.	Saves time in setting up network virtual services. Supports existing branch migration without hardware upgrade.
EasyQoS	Automation feature that creates an optimal end-to-end Quality-of-Service (QoS) chain for each link in the network.	Provides consistent QoS across the WAN and enterprisewide. Achieve toll-quality voice from any device, whether enterprise owned or user provided (BYOD).
Encrypted Traffic Analytics (ETA)	Allows the system to look for trends that could indicate a security threat in encrypted data traffic.	Detects malware, attacks, and other threats.
Network Health dashboard and client health dashboard	Assurance feature that gives a quick overview of the health of every network device and client on the network, wired or wireless.	Offers a general overview of the operational status of every network device provisioned from Cisco DNA Center. Any poorly connected devices will be highlighted with suggested remediation.
Device 360 Client 360	Assurance feature that displays device or client connectivity from any angle or context. Includes information on topology, throughput, and latency from different times and applications.	Provides a detailed view of the performance of any device or client over time and from any application context. Provides very granular troubleshooting in seconds.

Feature	Description	Benefits
Network time travel	Assurance feature that allows an operator to see device or client performance in a timeline view to understand the network state when an issue occurred.	Enables an operator to go back in time and see the cause of a network issue, instead of trying to re-create the issue in a lab.
Path trace	Assurance feature that allows the operator to visualize the path of an application or service from the client through all devices, and to the server.	Instantly performs a common, and critical, troubleshooting task that normally requires 6 to 10 minutes. The operator simply clicks on a client or application.
Aironet® Active Sensor	A compact network sensor designed to monitor your wired or wireless network.	Simulates real-world client experiences in order to validate wireless performance for critical venues and high-value locations such as conference halls and meeting rooms.
Machine learning algorithms	As network conditions change, context-aware baselining captures the relationship between metrics and constantly updates an optimal curve (regression) for performance. Precise issues can be identified when they deviate from this ever-changing baseline.	Updates the preferred performance curve in real time, as network conditions change. Issues raised are based on current and real network conditions, rather than a static model. The result is 75% fewer issues to troubleshoot.
Cisco DNA Center platform	A broad set of APIs, SDKs, and adapters that extend the capabilities of Cisco DNA Center to external applications, cross-architectural domains, systems and processes, and third-party devices.	Allows Cisco DNA Center to share network data and insights that can provide important intelligence related to business and IT operations. It also allows real-time control of the network in lockstep with business needs.

PTX-410 at 481885-86.

573. The demonstratives below, which were shown during the direct examination of Dr. Striegel, shows the grouping of top-level functions. Tr. 1367:4-1368:1.



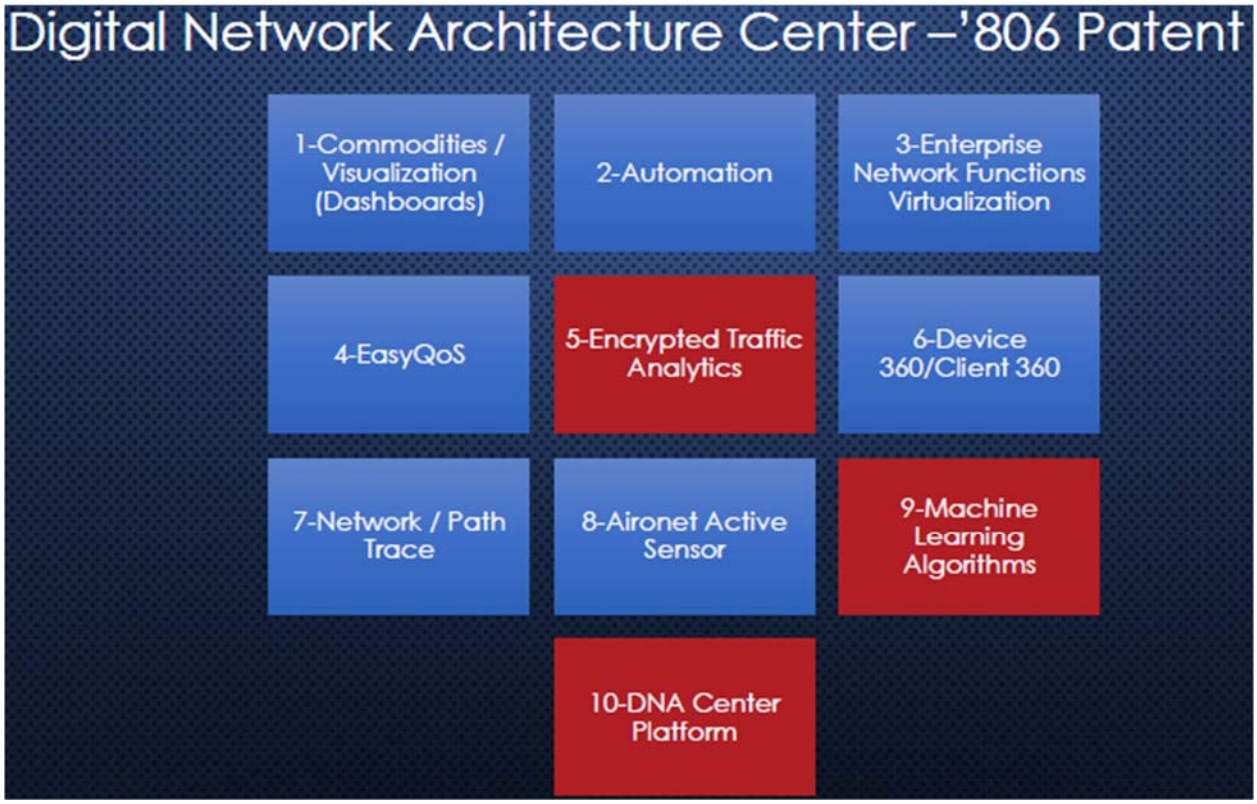


574. Group 2 covers Automatic Software Image Management and Automatic Plug and Play because they both cover automatic software management. Tr. 1367:16-20.

575. Group 7 cover Network Time Travel and Path Trace because they relate to the same sphere of operation. Tr. 1367:21-1368:1.

576. The remaining features identified by Cisco in PTX-410 at 481885-86 map directly to high-level functions as Cisco identified them. Tr. 1367:4-1386:1.

577. Of the ten top-level functions of the DNA, three are covered by the '806 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel and matched the infringement opinion of Dr. Mitzenmacher. Tr. 1368:2-16.



578. The '806 Patent relates to the Encrypted Traffic Analytics grouping because of the DNA's use of rules. Tr. 1368:2-13.

579. The '806 Patent relates to Machine Learning Algorithms grouping because of its usage of rules. Tr. 1368:2-13.

580. The '806 Patent relates to DNA Center Platform because of its usage and pushing of rules. Tr 1368:2-13.

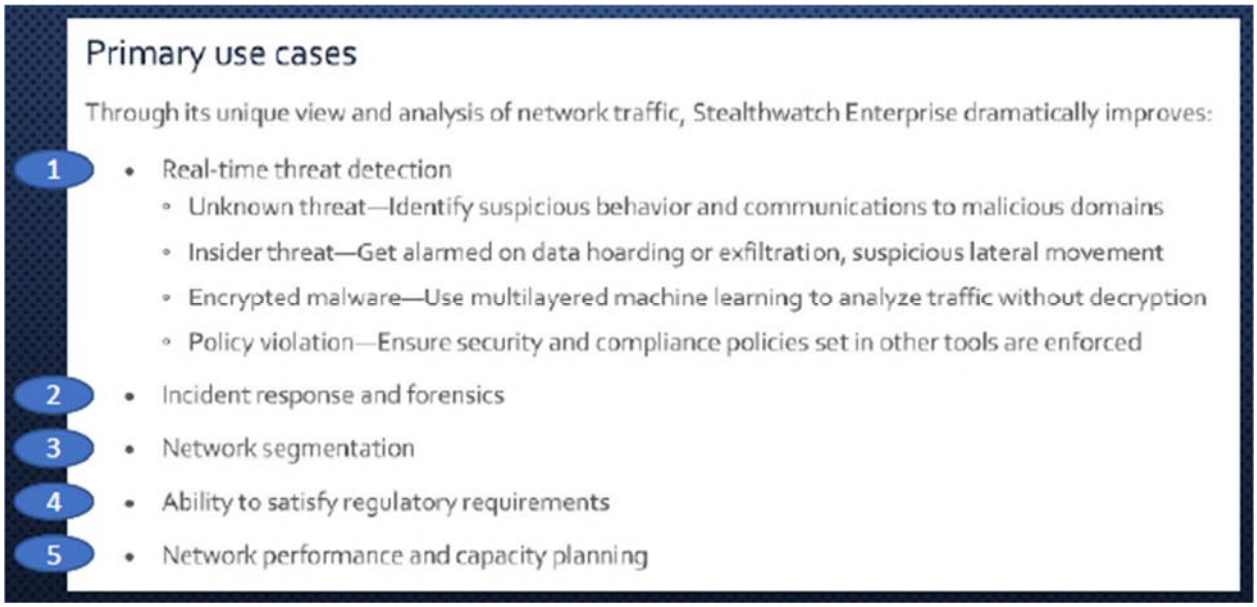
vii. Apportionment of Stealthwatch

581. Stealthwatch has five top-level functions when standardized by features and commodity components, which are shown on PTX-577 at 040007 and which is reproduced below. Tr. 1369:1-1370:2; PTX-577 at 040007.

- Real-time threat detection
  - Unknown threat—Identify suspicious behavior and communications to malicious domains
  - Insider threat—Get alarmed on data hoarding or exfiltration, suspicious lateral movement
  - Encrypted malware—Use multilayered machine learning to analyze traffic without decryption
  - Policy violation—Ensure security and compliance policies set in other tools are enforced
- Incident response and forensics
- Network segmentation
- Ability to satisfy regulatory requirements
- Network performance and capacity planning

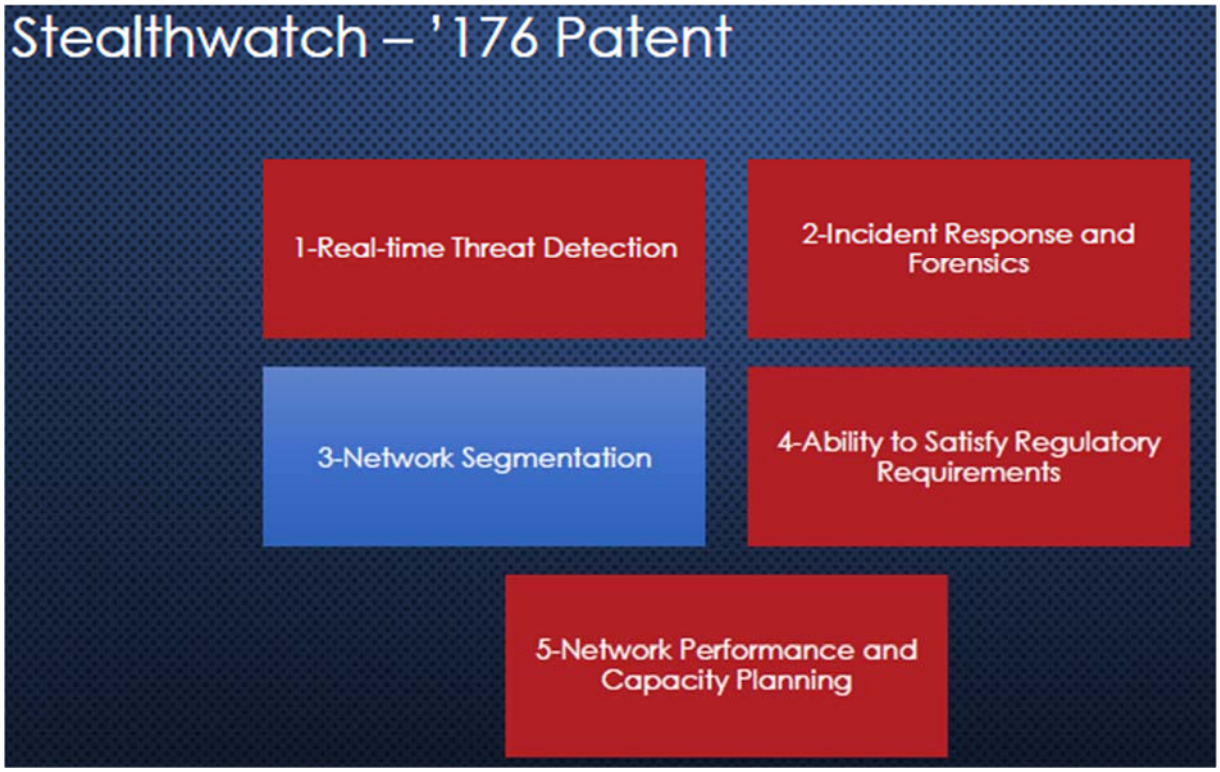
PTX-577 at 040007.

582. The demonstratives below, which were shown during the direct examination of Dr. Striegel, shows the grouping of top-level functions. Tr. 1369:1-1370:2.



583. The features identified by Cisco in PTX-577 at 7 map directly to high-level functions as Cisco identified them. Tr. 1369:1-1370:2.

584. Of the five top-level functions of Stealthwatch, four are covered by the '176 Patent, as shown in the demonstrative below that was shown at trial during the direct examination of Dr. Striegel. Tr. 1370:16-1371:1.



585. The '176 Patent relates to Real-time Threat Detection because it is necessary to extract the appropriate information from the log entries. Tr. 1370:16-21.

586. The '176 Patent relates to Incident Response and Forensics because it relates to material directly in the claims. Tr. 1370:16-22.

587. The '176 Patent relates to the Ability to Satisfy Regulatory Requirements because this relates to the benefits of operating the '176 Patent. Tr. 1370:16-24.

588. The '176 Patent relates to Network Performance and Capacity Planning because it is directly in the claims related to provisioning. Tr. 1370:16-1371:1.

I. Cisco Made Substantial Revenues from Its Sales of the Accused Products

589. Cisco made no showing, by government contract or otherwise, that any sales of Accused Products were used or manufactured for the United States Government with the authorization or consent of the United States Government. Tr. 1502:1-7.

590. Centripetal demonstrated that Cisco sells the infringing products as integrated systems, and that Cisco makes, uses and sells Switches, Routers and Firewalls embedded with and sold in combination with the infringing technology, whereas Cisco did not support its theory (*see* Findings of Fact, Section VIII(B)), accordingly the royalty base includes the following revenues of infringing systems, and does not include product revenues that were not infringing combinations.

591. Cisco's worldwide revenue for the Accused Products for the time period of approximately June 2017 to March 2023 is set forth in PTX-1958 at Schedule 5. These worldwide revenues are broken down as follows:

a) Catalyst 9000 Switch - $[redacted]

b) ASR Router - $[redacted]

c) ISR Router - $[redacted]

d) Adaptive Security Appliance - $[redacted]

e) ASA Subscription - $[redacted]

f) Firepower Appliance - $[redacted]

g) Firewall Appliance Subscription - $[redacted]

h) Firepower Management Center - $[redacted]

i) Digital Network Architecture - $[redacted]

j) Stealthwatch - $[redacted]

PTX-1958 at Schedule 5.

592. Cisco's total apportioned worldwide revenue for the Accused Products for the time period of approximately June 2017 to March 2023 is $[redacted]. PTX-1958 at Schedule 5. These apportioned worldwide revenues are broken down as follows:

a) Catalyst 9000 Switch - $[redacted]

b) ASR Router - $[redacted]

c) ISR Router - $[redacted]

d) Adaptive Security Appliance - $[redacted]

e) ASA Subscription - $[redacted]

f) Firepower Appliance - $[redacted]

g) Firepower Appliance subscription - $[redacted]

h) Digital Network Architecture - $[redacted]

i) Firepower Management Center - $[redacted]

j) Stealthwatch - $[redacted]

PTX-1958 at Schedule 5.

593. Cisco's United States revenue for the Accused Products for the time period of approximately June 2017 to March 2023 is set forth in PTX-1958 at Schedule 5.2. These United States revenues are broken down as follows:

a) Catalyst 9000 Switch - $[redacted]

b) ASR Router - $[redacted]

c) ISR Router - $[redacted]

d) Adaptive Security Appliance - $[redacted]

e) ASA Subscription - $[redacted]

f) Firepower Appliance - $[redacted]

g) Firepower Appliance Subscription - $[redacted]

h) Firepower Management Center - $[redacted]

i) Digital Network Architecture - $[redacted]

j) Stealthwatch - $[redacted]

PTX-1958 at Schedule 5.2.

594. Cisco's apportioned United States revenue for the Accused Products for the time period of approximately June 2017 to March 2023 is $[redacted], as set forth in PTX-1958 at Schedule 5.2. These apportioned revenues are broken down as follows:

a) Catalyst 9000 Switch - $[redacted]

b) ASR Router - $[redacted]

c) ISR Router - $[redacted]

k) Adaptive Security Appliance - $[redacted]

l) ASA Subscription - $[redacted]

m) Firepower Appliance - $[redacted]

n) Firepower Appliance Subscription - $[redacted]

o) Firepower Management Center - $[redacted]

p) Digital Network Architecture - $[redacted]

d) Stealthwatch - $[redacted]

PTX-1958 at Schedule 5.2.

595. For the products that are alleged to infringe two or more patents (i.e., Switches and Routers), the above revenues are counted only once. Tr. 1501; 2946.

596. Centripetal did not unduly delay in bringing suit, nor are there any other exceptional circumstances that militate against an award of prejudgment interest.

597. Prejudgment interest should be calculated on the amount of past damages from date the complaint was filed through the date of judgment. Prejudgment interest should also be calculated on those sales ordered by accounting that occur before the entry of a final judgment.

598. Prejudgment interest should be calculated at the prime rate and compounded quarterly to compensate Centripetal for Cisco's willful infringement of the Asserted Patents.

599. Post-judgment interest must be paid on all elements of the money judgment, including past damages, prejudgment interest and the accounting of sales, attorney's fees, enhanced damages and costs, and should be calculated from the time the judgment is entered by the Court to the time the payment is made.

J. Cisco Knew of the Asserted Patents and Centripetal Gave Notice of Its Infringement

600. Centripetal marks its products with the patent numbers shortly after each patent issues when the product practices the patent. Tr. 1203:12-1205:6; PTX-528.

601. The Asserted Patents issued on the following dates: the '806 Patent issued on December 1, 2015, the '176 Patent issued on January 31, 2017, and the '193 Patent issued on June 20, 2017. JTX-2-4.

602. When Centripetal met with Cisco in February 2016 and presented information about its RuleGATE product under NDA, including providing a live demonstration of its patented technology, Centripetal's product was marked with the '806 Patent. Tr. 1203:12-1205:6; 1212:17-1219:21; PTX-99, PTX-547, PTX-1136.

603. Centripetal develops new technology, files for patents covering that technology, and then incorporates that technology into its products for release. Tr. 315:3-316:5.

604. Centripetal's products practice the technology covered by the asserted claims of the Asserted Patents. Tr. 1381:13-1383:14; 1384:12-19; PTX-1215.

605. As of the end of June 2017, Centripetal's products were marked with the '806, '193, and '176 Patents, and have continuously been marked with those patent numbers. *See* Tr. 1203:12-1205:6; PTX-528.

606. Centripetal retained an investment banking firm called Oppenheimer & Co. in which Oppenheimer had a couple of meetings directly with Cisco about Centripetal in the November and December 2016 timeframe. Tr. 1234:19-25. Oppenheimer presented a presentation that Centripetal prepared that provided a comprehensive review of Centripetal's entire business. The presentation that included confidential architectural diagrams of Centripetal's patented products and had a slide entitled "Robust Patent Portfolio" which identified the '806 Patent. Tr. 1235-1238; DTX-1270.

607. Centripetal identified Cisco's infringement of the '806, '193 and '176 Patents on February 13, 2018 when it filed the Complaint. Dkt. No. 1.

K. Dates of First Infringement and the Hypothetical Negotiation

608. Both parties' experts agree that the date of the hypothetical negotiation is June 20, 2017. Tr. 1444-45, Tr. 2923:24-2924:1; 2933:1-6.

609. All Asserted Patents would be negotiated for licensing at the same time, because two of the four infringed patents ('193 and '806 Patents) had been granted and the '176 Patent were filed prior to June 20, 2017 and would have been known. JTX-2-4; Tr. 1444:6-1446:18.

610. Cisco's press release for the launch of ETA, DNA Center, and the Catalyst 9000 switches was dated June 20, 2017. PTX-1135.

611. The earliest date of first infringement and earliest start date of damages is June 20, 2017. Tr. 1515-16; Tr. 725; Tr. 2964 (Cisco's damages expert, Dr. Becker, agreeing that June 20, 2017 is "generally" when damages start). The start date for damages for the other Asserted Patents correspond with the dates of first infringement when the Accused Products for those Asserted Patents were released, as identified below.

612. The date of first infringement of Claims 18 and 19 of the '193 Patent is June 20, 2017 for the Catalyst 9000 Switches and ISR/ASR Routers. Tr. 1515:24-1516:2; PTX-1629.

613. The date of first infringement of Claims 9 and 17 of the '806 Patent is January 26, 2018 for the Catalyst 9000 Switches with DNA and the ISR/ASR Routers with DNA. Tr. 1516:8-18; PTX-1629.

614. The date of first infringement of Claims 9 and 17 of the '806 Patent is October 23, 2017 for the Firewalls with FMC. PTX-1629; *see also* Tr. 1515:2-1517:20.

615. The date of first infringement of Claims 11 and 21 of the '176 Patent is August 18, 2017 for the Catalyst 9000 Switches with Stealthwatch and the ISR/ASR Routers with Stealthwatch. Tr. 1516:3-7; PTX-1629.

L. Credibility of Witnesses for Damages

616. Cisco's expert for damages, Dr. Becker, took positions that established that his testimony was not credible.

617. Dr. Becker claimed that the reasonable royalty for the '193, '806, and '176, Patents was $934,323, despite all of Cisco's representations that security was a game changer for Cisco. DTX-1693 at 1; *see* Findings of Fact, Section II(E).

618. Cisco offers for sale and sells the Accused Products as integrated systems that provide network security functionality "of critical importance" to Cisco and its customers and that security was a top priority for Cisco's customers that was "driving another consecutive quarter of double-digit growth" for Cisco. *See, e.g.*, Tr. at 1453:22-1456:2, 1456:17-1459:9; 1462:16-1464:13, 1464:18-1467:11, 1472:17-25, 1499:18-1500:19, 1525:10-25; PTX-560, PTX-333; PTX-197; PTX-1507; PTX-1035.

619. Cisco markets and sells its products as a "cybersecurity architecture" and "as one product" based on Cisco's SEC statements, presentations, and technical marketing materials. *Id.* (explaining evidence such as PTX-1248 at 265-266; PTX-1507 at 494-495; PTX-560 at 768, 771); Tr. 440-441:14 (citing PTX-1260 at 849); PTX-197 at 196, 207.

620. Cisco's technical expert, Dr. Schmidt, confirmed that customers need Cisco's "comprehensive technique" and "[c]omprehensive set of products." Tr. 2130:7-20.

621. Despite the overwhelming evidence, as described above, Cisco contended that there was insufficient proof that its products were sold in the infringing combinations and thus properly counted in the royalty base. *See* Findings of Fact, Section VIII(A). As a result, Dr. Becker excluded from his proposed royalty base all revenues from the Catalyst 9000 Switches, ISR/ASR Routers, and Firewalls—the smallest saleable patent practicing units. *See* Findings of Fact, Section VIII(A). Despite an unlimited additional opportunity to support its claim that all revenues for the Accused Products were not sold as part of infringing combinations, Cisco was unable to produce any data justifying Dr. Becker's analysis. *See* Findings of Fact, Section VIII(A).

622. Dr. Becker's damages figure is objectively unreasonable and the product of unreliable methodology for various additional reasons.

623. For example, Dr. Becker's damages figure is less than the $3.86 million that Cisco stated was the cost of a ***single*** data breach. PTX-584 at 398.

624. Dr. Becker's damages figure is objectively unreasonable because it makes the effective royalty rate an infinitesimal fraction, which does not reflect a reasonable royalty that parties at a hypothetical negotiation would agree upon. Additionally, it is far lower than the agreed-upon rate from the Keysight License, highlighting its unreasonableness.

625. Dr. Becker's damages figure is unreasonably low because it is inconsistent with Cisco's acknowledgement that security was "the top IT priority for many of our customers," (PTX-333), such that Cisco would in fact find Centripetal's patented security solutions very valuable. Tr. 1455-1456.

626. Dr. Becker's damages figure is unreasonably low because it is inconsistent with Cisco's representation that it was unaware of any other licenses relevant to the technology of the Asserted Patents (Tr. 1477-79), which reinforces that no one was doing anything close to Centripetal's technology. This exclusivity justifies a higher value at the hypothetical negotiation.

627. Dr. Becker's contention that the Accused Products are not marketed and sold as integrated systems conflicted with Dr. Schmidt's testimony that "only those customers [that] are extremely looking forward to having their networks hacked" would fail to use Cisco's "comprehensive set of products." Tr. at 2130:7-20, 2131:12-22.

628. Dr. Becker's apportionment position was also unreasonable and unreliable because Dr. Becker made unsupported "huge reduction[s]." Tr. 3475:5-11.

629. After hearing Dr. Becker's testimony, the Court noted that Dr. Becker's apportionment theory "borders on the absurd" and that "[t]here's no way the Court will accept that analysis." Tr. 3473:21-3475:23.

630. Dr. Becker's apportionment position was also objectively unreasonable and unreliable because it was akin to arguing that air bags and seat belts are of no value unless deployed in an emergency. Tr. 3475:5-11.

631. Dr. Becker's analysis that the Accused Products were not the real source of the patented improvement, such that their revenues are not part of the royalty base, conflicted with the testimony of Cisco's engineers, Messrs. Llewallyn and Jones. Tr. 3475:4-23. For example, Mr. Llewallyn confirmed that the Catalyst 9000 Switch and ISR/ASR Router can quarantine malicious traffic in response to information from Stealthwatch. Tr. 2202:5-2203:2. The Accused Products are thus an integral part of the patented solutions and essential to delivering the benefits of the Asserted Patents to Cisco's customers.

632. Dr. Becker has no relevant or applicable opinion as he failed to update his reasonable royalty analysis to account for the increased damages period from 2017 to 2023 when Cisco updated its revenues. His opinion should thus be disregarded.

IX. FACTS RELATED TO WILLFUL INFRINGEMENT AND ENHANCEMENT OF DAMAGES

A. Cisco Willfully Infringes the Asserted Patents

633. Between 2015 and 2017, Centripetal and Cisco had numerous meetings and discussions about Centripetal's business, technology, products, and patents, and Centripetal did multiple demonstrations of its patent-practicing RuleGATE product for Cisco. *See* Findings, of Fact, Section II(C).

634. After Cisco executed the NDA, Centripetal and Cisco had several meetings, including with Cisco's technical and corporate development teams, where Centripetal provided multiple confidential demonstrations of RuleGATE and its patented technology. *See* Findings of Fact, Section II(C).

635. Centripetal disclosed substantial confidential information, including details about its patented technology and products, to Cisco during their meetings. *See* Findings of Fact, Section II(C).

636. In a WebEx meeting on February 4, 2016, Centripetal presented, *inter alia*, "detailed, highly sensitive, confidential and proprietary information about its patented technology and products," including its patented filter algorithms to prevent exfiltration ('193 Patent), correlation algorithms ('176 Patent), and rule swapping ('806 Patent). *See* Findings of Fact, Section II(C).

637. At that meeting, Cisco displayed interest in Centripetal's patented technology by asking questions regarding Centripetal's patents, filter technology, and algorithms. *See* Findings of Fact, Section II(C).

638. Contemporaneous documents confirmed these disclosures, such as emails to Cisco from Jonathan Rogers, Centripetal's VP of Operations at the time, noting that the Cisco team "hone[d] in on our filter technology and algorithms" and asked "questions on our patents." *See* Findings of Fact, Section II(C); PTX-102 at 1.

639. In another contemporaneous communication, Cisco Distinguished Engineer T.K. Keanini told his team that "What might be work [sic] exploration is to look at these algorithms they have . . . Again, knowing what patent offices will allow and not allow, I'd be very surprised if they were able to make claims on the algorithms themselves but we don't know until we study their claims." *See* Findings of Fact, Section II(C); PTX-134 at 3.

640. Centripetal and Cisco had further contact in 2016, including Centripetal's participation in the Cisco Live conference by Cisco's invitation. *See* Findings of Fact, Section II(C).

641. Later that year, Cisco received additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGATE functionalities covered by the Asserted Patents. *See* Findings of Fact, Section II(C).

642. After all of these detailed meetings with Centripetal, Cisco released its "network of the future" products on June 20, 2017, which incorporated Centripetal's patented technology. *See* PTX-1135 (Cisco's press release announcing technologies that infringe the '856 Patent

(Encrypted Traffic Analytics), '193 Patent (the rebuilt Catalyst 9000 Switches with new operating system), and '806 Patent (DNA); *see also,* Findings of Fact, Section II(C).

643. Even then, Cisco maintained interest in Centripetal. For example, in November 2017, Cisco's Senior Director of Cybersecurity Investments and Acquisitions, Karthik Subramanian, expressed interest in receiving more technical information from Centripetal, which Jonathan Rogers provided to him, including a "white paper explaining the intelligence led cloud service architecture for providers using our virtual enforcement points." *See* Findings of Fact, Section II(C); Tr. at 1245:8-1246:17.

644. Over an eighteen-month period when Cisco purported to be interested in a partnership, Cisco's employees were combing through Centripetal's website for additional information, accessing over 1,200 web pages over the course of 354 visits. *See* Findings of Fact, Section II(C).

645. Cisco, instead of becoming a distributor of Centripetal's technology, copied Centripetal's patented technology, after having numerous meetings with Centripetal and about Centripetal, its business, technology, products and patents. *See* Findings of Fact, Section II(C).

646. Cisco's revenues increased after its release of the infringing technology. Tr. 1607:22-1608:18, 3435:4-3438:24.

647. The repeated contact between the parties and their progression to signing an NDA—and continued contact after that—evidences Cisco's strong interest in Centripetal's patented technology. *See* Tr. 1019:2-18, 1020:16-1021:15, 1024:16-1026:18.

648. "The relationship between the parties is such that[,] . . . given the conducts and meetings and the similarity of the technology," Cisco could not have "infringed accidentally." *See* Tr. 3503:25-3504:12.

B. Credibility of Witnesses Regarding Willful Infringement

649. Centripetal presented two fact witnesses (Steven Rogers and Johnathan Rogers) and one expert witness (Dr. Eric Cole) to testify about the parties' interactions prior to this litigation. Tr. 256:8-260:18, 1212:17-1247:23, 1015:21-1028:12.

650. Steven Rogers testified about Cisco's first contact with Centripetal in 2015 when he was personally contacted by Pavan Reddy to learn about Centripetal's patented technology, which it viewed as a solution that "fit into the types of solutions [Cisco] needed for customers . . . that went beyond the offerings that Cisco had at the time." Mr. Reddy and Mr. Rogers had a follow-up meeting that same year, where Centripetal provided a demonstration of its system and explained why it was an effective method of cyber defense. Tr. 256:8-257:12. This testimony was unchallenged by Cisco.

651. Mr. Rogers also provided testimony that as a result of these meetings, on January 26, 2016, Centripetal and Cisco entered into an NDA. Tr. at 257:13-18. This testimony was unchallenged by Cisco.

652. Mr. Rogers testified that after Centripetal and Cisco executed the NDA the parties had had another meeting in February 2016. Trial exhibit PTX-547, a contemporaneous document dated at the time of the February meeting, was marked and Mr. Rogers testified that he "believe[d] it's the presentation that was provided to Cisco." Tr. 259:5-11. Referring to page 7 of PTX-547, Mr. Rogers testified that Cisco was provided information about Centripetal's patented filter algorithms, and that the system was patented. Tr. 260:5-18.

653. Jonathan Rogers confirmed Centripetal's meeting with and demonstration to Cisco in 2015. Tr. 1212:17-1213:15. Mr. Rogers also proved testimony regarding entering into an NDA with Cisco in early 2016, and the dated NDA was marked as PTX-99. Tr. 1213:16-1214:12.

654. Mr. Rogers provided detailed, credible testimony, supported by contemporaneous documents (PTX-547 and PTX-102), about the February 4, 2016, meeting where Centripetal presented information about its patented technology and products to Cisco in a WebEx meeting, including details of its patented technology for the Asserted Patents. Tr. 1215:14-1216:6, 1220:9-1224:22; PTX-547 at 389-91; PTX-102 at 1. For example, Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies 'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics." PTX-547 at 389-92; Tr. 1219:22-1222:25.

655. Mr. Rogers testified that during that meeting, Centripetal presented "detailed, highly sensitive, confidential and proprietary information about its patented technology and products," including its patented filter algorithms to prevent exfiltration ('193 Patent), correlation algorithms ('176 Patent) and Centripetal's patented technologies for detecting threats in encrypted traffic ('856 Patent), and rule swapping ('806 Patent). Tr. at 1219:15-1224:22; PTX-547 at 389-91.

656. Mr. Rogers also testified how Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies 'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics." PTX-547 at 389-91; Tr. 1219:22-1222:25. Centripetal also answered various questions about its patented technologies at the meeting. Tr. at 1225:12-16, 1227:9-18; PTX-102 at 1.

657. Mr. Rogers testified that Centripetal and Cisco had further follow-up meetings and communications after the February 2016 WebEx meeting, demonstrating Cisco's continued

interest in Centripetal. Tr. 1233:20-1234:9. For example, in July 2016, Cisco invited Centripetal to be a technology partner at its Cisco Live conference, where Centripetal again presented its patented solution. Tr. at 1234:10-16, 1297:23-1299:9. In December 2016, Oppenheimer presented to Cisco additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGATE functionalities covered by the Asserted Patents. Tr. at 1235:11-1236:21, 1237:25-1238:19, 1242:11-1243:10; DTX-1270 at 1, 25, 27-28, 30.

658. For every fact about Centripetal's interactions with Cisco that Steven Rogers and Jonathan Rogers testified to at trial, there were a number of contemporaneous documents to support their trial testimony.

659. Dr. Cole provided expert insight and opinions into these types of interactions from one skilled in the art. Tr. 1015:21-1028:12.

660. Cisco presented two fact witnesses at trial that attempted to recharacterize the contemporaneous exhibits regarding Centripetal's and Cisco's meetings – Timothy (TK) Keanini and Karthik Subramanian. Tr. 2810:10-2852:28. Neither of these two witnesses was credible.

661. Mr. Keanini was put on the stand to explain his February 5, 2016, email the day after the WebEx meeting with Centripetal. He wrote an internal email to his team stating:

> It appears that most of their **intellectual property** lays in the claim that given 'n' amount of signatures (they call them rules) they are able to instrument them in an inline device. . . . What might be work [sic] **exploration is to look at these algorithms** they have and how general purpose they may be for data synthesis – high performance set theoretical functions. Again, **knowing what patent offices will allow and not allow**, I'd be very surprised if they were able to make claims on the algorithms themselves but **we don't know until we study their claims**.

PTX-90 (emphasis added); *see also* Tr. 2814:25-2815:3 (Mr. Keanini testifying that "The word 'work' should be 'worth.'").

662. During cross examination, Mr. Keanini testified that he had no memory of Centripetal talking about their patents at the meeting. Tr. 2818:15-22. When shown page 7 of the meeting presentation marked PTX-547 that discussed Centripetal's patents, he changed his testimony and said they only discussed their patents at a high level. Tr. 2818:23-2820:10.

663. When asked about the first sentence of his email marked as PTX-90 about intellectual property, he responded as follows:

> Q. So when you're talking about intellectual property you're talking about patents, right?
>
> A. No. Again, I may have chosen the wrong word here. I was just -- in that first paragraph I was just trying to establish that I was paying attention at the meeting and that I understood what they did. I didn't really mean their intellectual property. I meant the stuff they said they did in that demo.

Tr. 2821:4-10.

664. When asked about the second sentence where it stated it might be worth exploring Centripetal's algorithms, Mr. Keanini testified Centripetal "didn't really talk about their algorithms." Tr. 2821:19-2822:9.

665. When asked about his statement about the patent office and studying Centripetal's claims, Mr. Keanini testified that he "was just trying to express the fact that I wasn't -- I didn't want to come off as arrogant." Tr. 2822:16-2823:4.

666. Cisco also presented Mr. Karthik Subramanian to testify about the February 2016 meeting between Centripetal and Cisco. During his deposition in this case, he had no memory of Centripetal or any meeting with Centripetal. At trial, he said he had his memory refreshed by the

documents and provided testimony about the documents. Tr. 2849:17-2850:24. However, even at trial he could not remember if he actually attended the February 2016 meeting.

> Q. And you said you don't recall going to the February 4th meeting one way or the other. You may have gone, you just don't recall, correct?
>
> A. Yes. You know, I don't recall the specifics of that, you know. It was organized by my team. I think more than likely I was part of that meeting as well, I just don't remember specifics.

Tr. 2851:7-13; *see also* 2851:14-24.

667. Mr. Subramanian's testimony was pure speculation and was not credible.

C. Cisco's Willful Infringement and Litigation Tactics Justify Enhanced Damages

668. Cisco has existed since the 1980s and touts itself as the world's largest networking equipment company. PTX-576 at 991. It has enjoyed strong revenues, including increased revenues after releasing Centripetal's patented technology as its own. Tr. 1607:22-1608:18, 3435:8-3438:24; *see also,* PTX-1958.

669. Cisco deliberately copied Centripetal's patented technology based on the extensive confidential information that it received, the multiple demonstrations of the patent-practicing RuleGATE, Centripetal's patents, and its own monitoring of Centripetal. *See* Findings of Fact, Sections II(C), VIII(A).

670. Cisco strategically continued discussions with Centripetal and entered into an NDA to learn more about Centripetal's patented technology, pretending to have interest in a partnership.

671. Cisco did not offer evidence that it formed a good faith belief in invalidity or non-infringement of any Asserted Patent when it learned about Centripetal's patents.

672. Cisco's infringement has been ongoing for about six years, since June 2017 at the earliest.

673. Centripetal sued Cisco for patent infringement in February 2018. Dkt. No. 1. Cisco then dragged this litigation out for years using a variety of tactics.

674. Cisco engineered delays so as to avoid litigating the case until over one and a half years later in September 2019—which is more than the average time the Court normally takes to resolve patent cases through trial. Dkt. No. 68; *see also* Dkt. No. 67 (9/11/2019 Hearing Tr.) at 18:7-8 (the Court noting it "normally resolves patent cases within a year"). Cisco refused to convene a Rule 26(f) conference. Dkt. No. 402-1, Ex. 1. It then filed a partial motion to dismiss—which it ultimately withdrew (Dkt. No. 188)—but in the interim Cisco leveraged its pending motion as a *de facto* stay of the entire case, claiming that "its obligation to respond to the remaining claims . . . is deferred pending resolution" of the motion. Dkt. No. 38 at 2, n.1.

675. Cisco then filed three staggered waves of IPR petitions beginning in July 2018, five months after the complaint was filed, to maximize the IPR resolution timeline. *See* Dkt. No. 57. Several months later, in September 2018, Cisco moved to stay this action pending resolution of the IPRs, which the Court granted. Dkt. Nos. 45, 58.

676. Over Cisco's opposition, the Court granted Centripetal's Motion to Lift the Stay in September 2019. Dkt. No. 68. At the time, the Court noted the following concerns:

> This Court normally resolves patent cases within a year of when they're filed. The case has already been pending for a year and a half . . . . ***particularly this form of patent -- that is, computer programs -- has a shelf life, a very short shelf life. And I always tell the attorneys who are fighting over these cases, that by the time they finish litigating it, it may well be obsolete, and that's the problem I'm facing here. Obviously, security in this area is very much at the forefront of what people are seeking to develop at this time. So this area is bound to be extremely competitive, thus making the shelf life of the patents that much less. And I don't agree that you can necessarily resolve the plaintiff's problems by money damages***. When you're trying to enter a field so competitive as this, when you're delayed from being

> able to do it by alleged infringement, that's going to hamper the efforts for a new entity trying to enter the field . . . the Court should do everything it can do to encourage people to enter this field and to resolve disputes of this nature in as timely a manner as possible.

Dkt. No. 67 (9/11/2019 Hearing Tr.) at 18:4-19:11 (emphasis added).

677. Upon lifting the stay, the Court set trial for April 2020. Dkt. No. 74.

678. In March 2020, the Court asked the parties whether, in view of the fact that jury trials may be postponed due to COVID-19, the parties would agree to a bench trial in order to uphold the April 2020 trial date. Dkt. No. 402-3, Ex. 3 at 1-2.

679. Centripetal notified the Court that only "if the trial of this matter starts as scheduled on April 7, 2020, Centripetal will waive a jury and proceed with a bench trial." Dkt. No. 402-3, Ex. 3 at 1.

680. Cisco agreed to a bench trial, but sought to leverage the uncertainty of the pandemic by requesting a continuance "until the health issues related to Covid19 have passed." Dkt. No. 402-4, Ex. 4 at 2.

681. The Court convened a conference and, responding to Cisco's request, delayed the start of a bench trial to May 2020. Dkt. No. 402-5, Ex. 5 (3/12/2020 Hearing Tr.) at 3:2-12. During that conference, the Court expressed "concern[] about the length of the postponement" and later observed that "[w]e can't just keep postponing indefinitely" due to "the importance of this case being tried as soon as possible." Dkt. No. 402-5, Ex. 5 (3/12/2020 Hearing Tr.) at 2:22-25, 5:4-9.

682. Notwithstanding the Court's concerns about delay, Cisco moved to delay trial indefinitely until all could "safely" appear in court and to oppose proceeding by videoconference. Dkt. No. 387. The Court denied this motion and stressed the importance of

"resolv[ing] the matter with a sense of urgency" and "proceed[ing] expeditiously with the resolution of this case." Dkt. No. 406 at 2.

683. Despite the Court's repeated concerns, since the Court lifted the initial stay in October 2019 Cisco has moved four more times to stay, continue, sever, and/or bifurcate some or all issues in this case so as to delay final resolution. Dkt. Nos. 248, 387, 664, 687.

684. Cisco presented no evidence of remedial action, such as trying to design around the Asserted Patents. For about six years now, it has simply persisted in infringing while delaying resolution of Centripetal's claims.

685. Cisco continues to infringe the Asserted Patents to this day.

686. Cisco engaged in other inappropriate litigation tactics besides delay. In particular, it engaged in obfuscation and made misleading representations to the Court at the bench trial—but the record reflects that Cisco was unable to slip such representations by the Court. For example:

a. During Dr. Moore's cross, Cisco improperly conducted a product-to-product comparison and resisted Dr. Moore's questions to clarify a hypothetical diagram designed by counsel (Tr. at 355:15-361:11);

b. Cisco omitted portions of deposition testimony during an impeachment attempt (Tr. 377:11-379:19);

c. Cisco artificially limited cross-examination to a narrow embodiment to attempt to get more favorable testimony, which was an inaccurate characterization of Centripetal's allegations (Tr. 786:19-792:24);

d. Cisco impermissibly confusing and conflating issues by raising validity and damages issues during cross-examination relating to infringement (Tr. 1058:3-1059:10, 1061:4-1062:16, 1069:9-15);

e. Cisco used "misleading" questioning to misrepresent an Accused Product (Tr. 1535:18-1540:13);

f. Cisco attempted to assert that the accused products after 2017 were the same as the predecessor products represented in documents from 2012 (Tr. 1890:2-1893:3); and

g. Cisco attempted to assert a functionality added in 2017 in the Catalyst 9000 Switch was unchanged from functionality described in various documents about various products from 2011 (Tr. 3079:20-3082:6).

687. Cisco improperly attempted to supplement its poor record with fact witness declarations submitted with its post-trial briefing, well after the close of evidence. *See* Dkt. Nos. 626-1, 626-2.

688. Cisco again attempted to supplement the record before the Rule 63 Hearing (Dkt. No. 691), despite that the Court had already invited the parties to identify months earlier if there was discovery or "updated information" that should be accounted for in the case schedule leading up to the hearing (as Centripetal did, in obtaining a stipulation to updated damages figures). Dkt. No. 675 (1/25/2023 Hearing Tr.) at 28:11-16. Instead, Cisco waited until a few days before the parties' trial briefs were due before seeking to file its motion to supplement the record with approximately ***400 pages*** of material, not sponsored by any witness.

689. Before the Court ruled on Cisco's motion to supplement, Cisco simply quoted from one of the documents subject to its motion in its trial brief to attempt to inject language into the record regardless of what the Court would ultimately order. Dkt. No. 698 at 10.

690. Cisco also cited to portions of exhibits that were not admitted in its trial brief but that it also did not formally request to add to the record in its motion to supplement. *Compare* Dkt. No. 698 at 20 (citing DTX-3 at 4824-30, 4781-94), 26 (citing DTX-1 at 1330-35) *with* Dkt. No. 643 (Final Joint Admitted Trial Exhibit List) at 5.

691. Cisco's positions generally demonstrated a lack of credibility and were inconsistent with Cisco's documents and fact witness testimony. Centripetal presented credible evidence that Cisco could not and did not rebut.

X. FACTS RELATED TO INJUNCTIVE RELIEF

692. Centripetal seeks a permanent injunction enjoining Cisco from making, using, offering for sale, selling, and/or importing its Firewalls.

693. Centripetal practices the Asserted Patents. *See* Findings of Fact, Section III.

694. Centripetal and Cisco directly compete. *See* Findings of Fact, Section VIII(C).

695. Cisco knew of the '806 Patent before the filing of Centripetal's Complaint, as early as February 2016. *See* Findings of Fact, Sections II(C-D), VIII(J), IX(A). Cisco received notice of the '806, '176, and '193 Patents on February 13, 2018 with the filing of the Complaint. *See* Findings of Fact, Section VIII(J). Cisco received notice of the '856 Patent on March 29, 2018 when Centripetal filed its Amended Complaint. *See* Findings of Fact, Section VIII(J).

696. Cisco has not offered evidence that it has designed around or ceased to infringe any Asserted Patent. Its infringement is ongoing.

697. Centripetal has suffered reputational harm because Cisco claimed Centripetal's position at the forefront of the market. *See, e.g.*, Tr. at 1209:12-1210:20, 1246:19-1247:19

(Jonathan Rogers' testimony); Tr. 1331:15-1332:2 (Centripetal's VP of Sales testifying about encountering Cisco in the marketplace); Tr. 1606:12-1608:18, 1608:19-1609:19 (Centripetal's expert, Dr. Malackowski, explaining the negative impacts Centripetal suffered due to Cisco's improper first-to-market claim and "me-too followers" entering the market after Cisco began infringing); *see also* Tr. at 3464:8-14 (Cisco revenues increased after the release of infringing technology).

698. As the Court previously observed, patents in extremely fast-moving fields such as cybersecurity have "a shelf life," and excessive delay in the resolution of cases impacts a patentee's ability to capitalize on the benefits of the early period of its hard-earned patent monopoly. *See* Dkt. No. 67 (9/11/2019 Hearing Tr.) at 18:4-19:11.

699. Cisco's extensive delays in this case irrevocably diminished Centripetal's ability to benefit from the initial monopoly over its patented technology granted by the Patent Office, because Centripetal had to compete against its own technology in the marketplace for years while Cisco simultaneously continued to infringe and continued to push out the date on which Cisco would have to take a license. Essentially, Cisco forced Centripetal into limbo in the marketplace, refusing to allow Centripetal's infringement claims to be resolved while continuing to leverage its unearned position at the forefront of security innovation, during the period of time most crucial to a small company.

700. As a large company with diverse product offerings that has historically focused on networking hardware as opposed to security innovation (*see* Findings of Fact, Sections II(B)-(D)), Cisco would not suffer from the Court enjoining the making, using, offering for sale, selling, and/or importing of its Firewalls.

701. Centripetal has a scalable business model and is capable of meeting market demand for its patented security technology. Tr. 1248:5-19.

CONCLUSIONS OF LAW

I. CLAIM CONSTRUCTION

1. Claim construction is a matter of law for the Court. *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 389-90 (1996).

2. The Court incorporates by reference the Claim Construction Order and applies those constructions for purposes of determining infringement and validity.

3. The parties agreed on certain constructions, and the Court construed additional terms. A summary of the claim constructions for the Asserted Patents is below:

Term	Agreed Construction	Patent
rule	a condition or set of conditions that when satisfied cause a specific function to occur	'176 Patent
log entries	notations of identifying information for packets	'176 Patent

Dkt. No. 202 at 9.

Term	Court's Construction	Patent(s)
preambles	limiting	all Asserted Patents
packets	plain and ordinary meaning in the context of the claim in which the term appears	all Asserted Patents
correlate, based on the plurality of log entries	packet correlator may compare data in one or more log entries with data in one or more other log entries	'176 Patent
responsive to correlating	plain and ordinary meaning	'176 Patent
generate, based on the correlating, one or more rules	plain and ordinary meaning	'176 Patent

Dkt. No. 202 at 22.

II. INFRINGEMENT

A. Direct Literal Infringement

4. There are two types of direct infringement: (1) "literal infringement" and (2) "infringement under the doctrine of equivalents." In order to prove direct infringement by literal infringement, Centripetal must prove by a preponderance of the evidence that Cisco made, used, sold, offered for sale, and/or imported in the United States a system that meets all of the requirements of a claim during the time the Asserted Patent was in force. 35 U.S.C. § 271(a). A claim for patent infringement is proven by a preponderance of the evidence when infringement was more likely than not to have occurred. *Advanced Cardiovascular Sys., Inc. v. Scimed Life Sys., Inc.*, 261 F.3d 1329, 1336 (Fed. Cir. 2001). There are two steps: (1) the court determines the meaning of the asserted patent claims, and (2) the fact-finder determines whether the accused system infringes the claim as construed. *Id.*; *see also Cole v. Kimberly-Clark Corp.*, 102 F.3d 524, 528 (Fed. Cir. 1996). To establish literal infringement, each and every limitation of the asserted claim must be found in the accused system. *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling USA, Inc.*, 699 F.3d 1340, 1356 (Fed. Cir. 2012).

5. Unless construed, claim terms are given their plain and ordinary meaning as understood by a skilled artisan. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (*en banc*). Claims are only narrowed from their plain and ordinary meaning through disclaimer if statements during prosecution that are "so clear as to show reasonable clarity and deliberateness" and "so unmistakable as to be unambiguous evidence of disclaimer." *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1325 (Fed. Cir. 2003) (citations omitted). Statements that are ambiguous or amenable to multiple reasonable interpretations to not establish prosecution disclaimer. *See Tech. Props. Ltd. v. Huawei Techs. Co.*, 849 F.3d 1349, 1357-58

(Fed. Cir. 2017) (citing *Mass. Inst. of Tech. v. Shire Pharms., Inc.*, 839 F.3d 1111, 1119 (Fed. Cir. 2016)). "The party seeking to invoke prosecution history disclaimer bears the burden of proving the existence of a clear and unmistakable disclaimer that would have been evident to one skilled in the art." *Shire*, 839 F.3d at 1119 (citation and quotation marks omitted). This is a high burden for Cisco to prove.

6. Claims "must be construed in the identical way for both infringement and validity." *Kimberly-Clark Corp. v. Johnson & Johnson*, 745 F.2d 1437, 1449 (Fed. Cir. 1984); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1279 (Fed. Cir. 1988) ("Having construed the claims one way for determining their validity, it is axiomatic that the claims must be construed in the same way for infringement.").

7. A defendant directly infringes by offering to sell or selling a system that is designed to be "altered or assembled" after purchase, and infringes once altered or assembled. *See High Tech Med. Instrumentation, Inc. v. New Image Indus., Inc.*, 49 F.3d 1551, 1556 (Fed. Cir. 1995) ("Of course, if a device is designed to be altered or assembled before operation, the manufacturer may be held liable for infringement if the device, as altered or assembled, infringes a valid patent.").

8. That certain system components are available for sale separately does not defeat infringement, particularly when a defendant "advertises and sells all the accused products" as part of a "system" and frequently highlights the compatibility between those separately sold elements. *See, e.g.*, *Immersion Corp. v. Sony Computer Entm't Am., Inc.*, No. C 02-0710 CW, 2005 U.S. Dist. LEXIS 4777, at *16-17 (N.D. Cal. Jan. 10, 2005) (verdict supported by substantial evidence because defendant sold the accused consoles, controllers, and games for end-users to assemble). Additionally, a defendant cannot escape direct infringement when it

"does not dispute that it sells the separate components that, if attached together, may infringe the patent." *St. Clair Intell. Prop. Consultants, Inc. v. Toshiba Corp.*, No. 09-354-LPS, 2014 WL 4253259, at *3 (D. Del. Aug. 27, 2014) (following *Immersion* and denying motion for summary judgment of non-infringement because "direct infringement may be found where one sells or offers to sell all of the components of a claimed system, even if the components are sold separately and are required to be assembled by the customer").

9. In another example, a district court explained that "where an alleged infringer sells 'all of the elements of the patented combination as a single, albeit disassembled, unit,' reasonable [fact finders] may find that the defendant sells a complete system and thus infringes." *Chamberlain Grp., Inc. v. Techtronic Indus. Co.*, 315 F. Supp. 3d 977, 1001-02 (N.D. Ill. 2018), *aff'd in part, vacated in part, rev'd in part on other grounds*, 935 F.3d 1341 (Fed. Cir. 2019). This is consistent with 35 U.S.C. § 271(a), which only states that one not liable for making or selling less than a complete invention, because, here, Cisco is indeed selling a complete invention. In *Chamberlain*, the defendant directly infringed based on "evidence that the Ryobi [garage door openers ("GDOs")] and the Ryobi battery are configured to fit and operate together, and that both the GDOs' packaging and a video on the Ryobi website suggest coupling the GDO and the battery." *Id.* Another court found direct infringement for selling separate fluid tanks that customers assembled into an infringing structure. *EBS Auto. Servs. v. Ill. Tool Works, Inc.*, No. 09-cv-996 JLS (MDD), 2011 WL 4021323, at *5-6 (S.D. Cal. Sept. 12, 2011) (citing *High Tech Med. Instrumentation*, 49 F.3d at 1556) and noting "the patent laws do not allow a manufacturer to avoid infringement simply by selling a disassembled device that would infringe on assembly").

10. A defendant also directly infringes system and computer readable media claims when it makes, offers for sale, or sells a device where the application code for the infringing functionality is already present on the device. *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1205 (Fed. Cir. 2010) ("The code for proactive scanning was 'already present' in Defendants' accused products when sold.") The Federal Circuit has established that "[t]he fact that users needed to 'activate the functions programmed' by purchasing keys does not detract from or somehow nullify the existence of the claimed structure in the accused software." *Id.*; *Fantasy Sports Props., Inc. v. Sportsline.com, Inc.*, 287 F.3d 1108, 1118 (Fed. Cir. 2002) ("[A]lthough a user must activate the functions programmed into a piece of software by selecting those options, the user is only activating means that are *already present in the underlying software*.") (emphasis in original).

11. The Federal Circuit has explained that the *Secure Computing* line of cases is not narrowly limited to claims drafted with "for performing" terminology. *INVT SPE LLC v. Int'l Trade Comm'n*, 46 F.4th 1361, 1373-74 (Fed. Cir. 2022) ("[W]e see very little significance in the difference between a limitation that might recite 'a data obtaining section for demodulating and decoding' (*Finjan*-style) and one that recites 'a data obtaining section that demodulates and decodes' . . . for determining on which side of the capability/actual-operation line the claims fall.").

12. System and computer readable media claims do not require evidence of actual use after sale to be infringed, unlike method claims (which are not at issue here) where plaintiffs must prove performance of every step. *Secure Computing Corp.*, 626 F.3d at 1204.

13. *Deepsouth Packing v. Laitram*, 406 U.S. 518 (1972), cited by Cisco, is inapplicable to this case because the Federal Circuit has explained that "*Deepsouth* was intended

to be narrowly construed as applicable only to the issue of the extraterritorial effect of the American patent law." *Paper Converting Machine Co.v. Magna-Graphics Corp.*, 745 F.2d 11, 17 (Fed. Cir. 1984); *see also Deepsouth*, 406 U.S. at 531. There is no such consideration here.

14. Centripetal must prove, and has proven, that Cisco directly infringes by a preponderance of the evidence. *See* Findings of Fact, Sections V(A), VI(A), and VII(A).

15. Cisco does not dispute that it offers to sell and sells each of the Accused Products in the United States, which are acts of direct infringement under 35 U.S.C. § 271(a). *See also* Findings of Fact, Section VIII(B).

16. Cisco uses and tests the Accused Products in the United States, which are acts of direct infringement under 35 U.S.C. § 271(a). *See* Findings of Fact, Section VIII(B); *see also NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1317 (Fed. Cir. 2005) (system claim infringed when system put into service); *Segan LLC v. Zynga Inc.*, No. 11-670-GMS, 2013 WL 12156529, at *1 n.1 (D. Del. May 2, 2013) (internal use of accused product infringes system claims).

17. Cisco also makes the Accused Products by developing and compiling the infringing software code in the United States, which is an act of direct infringement under 35 U.S.C. § 271(a). *See* Findings of Fact, Section VIII(B).

18. Applying this Court's claim construction and based on the facts and expert evidence presented at trial, Centripetal has proven by a preponderance of the evidence that the Accused Products literally infringe the Asserted Claims of the Asserted Patents.

i. Centripetal Has Proven Direct Infringement of the '193 Patent

19. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 18 and 19 of the '193 Patent by making, using, selling, offering for sale and/or

importing the Catalyst 9000 Switch in the United States. *See* Findings of Fact, Section V(A)(i)-(ii).

20. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 18 and 19 of the '193 Patent by making, using, selling, offering for sale and/or importing the ISR/ASR Router in the United States. *See* Findings of Fact, Section V(A)(i)-(ii).

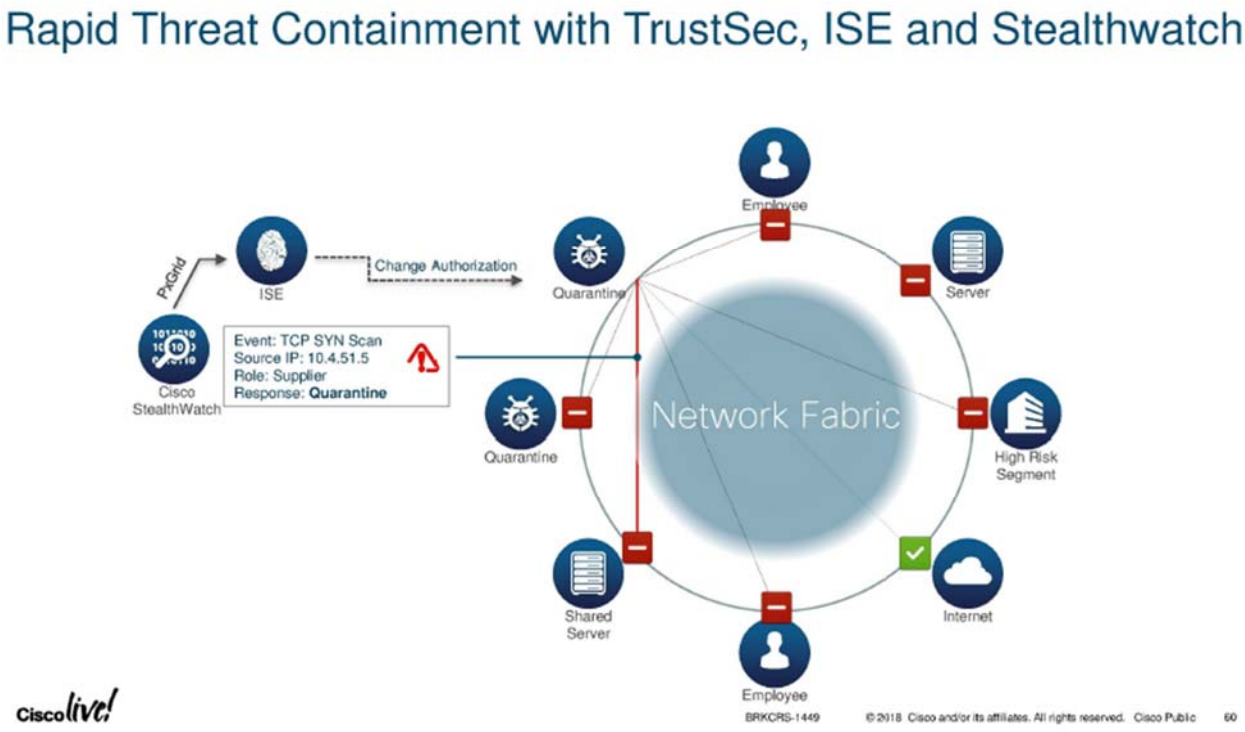
21. Dr. Crovella advanced two theories in his non-infringement opinion. First, that the function which is referred to as a "quarantine" blocks all traffic from a source computer and does not block a "particular data transfer," as required by the language in the claim. Second, he averred that Stealthwatch, using NetFlow, cannot identify exfiltrations until it is too late to drop the packet.

22. As to the first theory, Dr. Crovella admitted on cross-examination to the infringing process. This testimony, coupled with Cisco's technical information from PTX-1284 and PTX-1326, prove that the Catalyst 9000 Switch and ISR/ASR Router measure the vulnerability level of individual network risk and assign roles to groups of devices based on this analysis. Walking through the operation of the Catalyst 9000 Switch and ISR/ASR Router illustrates that they meet the functionality required by the Asserted Claims.

23. The Catalyst 9000 Switch and ISR/ASR Router can assign "roles" to a specific endpoint computer or a group of endpoint computers. PTX-1326 at 011. As a general example, the Cisco system operates by limiting a computer or group of computers located in a first network from accessing sensitive data in a protected network, while simultaneously allowing unsensitive data to be accessed. In this manner, packets from the computer in the first network may be allowed to access unprotected resources on the larger internet, but would be restricted

from transmitting packets containing secure information. *See* Findings of Fact, Section V(A)(i) and (ii)(c)-(f).

24. This is shown in Cisco's technical documentation, PTX-563:



PTX-563 at 415.

25. The Catalyst 9000 Switch and ISR/ASR Router are the specific network devices used to institute this packet filtering system. In their operation, the Catalyst 9000 Switch and ISR/ASR Router receive different portions of packets from a first computing network. PTX-1276 at 216. The SGT that is attached to each packet is based on the role and/or privileges that is assigned to that specific endpoint computer or group of computers. Therefore, SGTs, at their most basic level, are assigned to packets and govern the particular types of data transfers that are allowed for the computer or group of computers. The assignment of SGTs to packets is part of the quarantine or segmentation process. *See* Findings of Fact, Section V(A)(i) and (ii)(c-f).

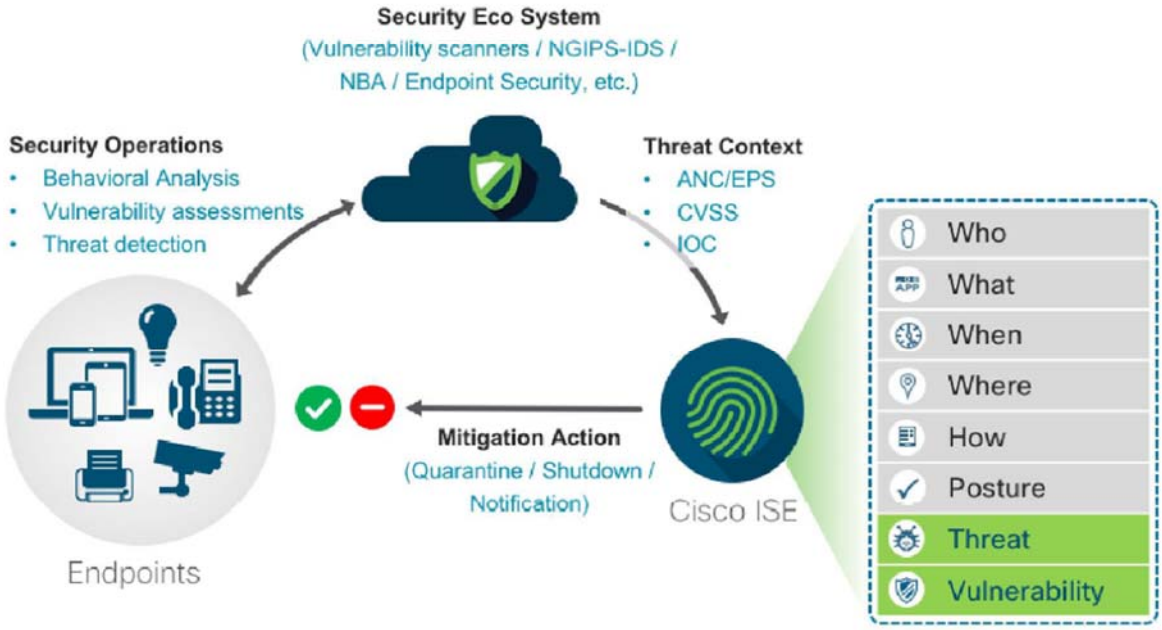
26. The Catalyst 9000 Switch and ISR/ASR Router utilize specialized rules, known as SGACLs, that deal specifically with forwarding and dropping packets based on what type of SGT is attached to the packet. These SGACLs prevent particular types of data transfers from one network to a second network, but allow traffic from one network to a third network. As Cisco's documentation states the Catalyst 9000 Switch and ISR/ASR Router will selectively block network traffic when "[d]evices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications." SGACLs are analyzed on both ingress and egress. The Catalyst 9000 Switch and ISR/ASR Router can then selectively block network traffic based on whether the data transfer is allowed to a particular network or not. *See* PTX-1390 at 86. *See* Findings of Fact, Section V(A)(i) and (ii)(c-f).

27. Centripetal's expert, Dr. Mitzenmacher, used PTX-1326 to confirm that Cisco's quarantine rule operates with this rule-based segmentation functionality. Moreover, technical documents, such as Cisco's Rapid Threat Containment Guide, confirm that the Catalyst 9000 Switch and ISR/ASR Router are programmed to "manually or automatically change your user's access privileges when there's suspicious activity, a threat or vulnerabilities discovered." Tr. 527:4-17; PTX-1326 at 011. Accordingly, the SGACL functionality within the Catalyst 9000 Switch and ISR/ASR Router contain malware infected computers by blocking "access to critical data while their users can keep working on less critical applications." PTX-1326 at 011. Thus, the Cisco system operates by blocking packets affiliated with a particular type of data transfer to a protected resource on a first network while allowing packets unaffiliated with a protected type of data transfer to be transmitted to a second network. In this manner, the technical documents confirm that the accused products utilize "packet filtering-rules" that operate to prevent "a particular type of data transfer" from a first to a second network. This functionality is shown by

text and diagram included in Cisco's technical document that outlines the operation of the rapid threat containment feature:

With integrated network access control technology, you can manually or automatically change your users' access privileges when there's suspicious activity, a threat. or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.

1.6.2 How does Rapid Threat Containment work



See PTX-1326 at 011 (showing infected endpoints can be denied access to certain types of data while being allowed access to other types of data).

28. This functionality confirms that SGTs are applied to groups and tag network traffic and the Catalyst 9000 Switch and ISR/ASR Router enforce those policies by analyzing the packets and their respective SGTs and applies different "operators," such as permit/deny, to those packets based on the associated packet SGTs. Cisco's infringement expert, Dr. Crovella, on cross examination confirmed that the accused products perform the functionality required to infringe the claims:

> Q. . . .So we have multiple steps. First, the SGT tag is checked to see if it's present, right?
> A. That's right.
> Q. Then, if the SGT tag is present and it says, "quarantine," then a quarantine policy is applied, correct?
> A. That's right.
> Q. If the quarantine policy is applied, you check the destination, and if the destination is a protected resource in which it says, do not allow this packet to go there, it will prevent the data transfer from going to that destination, correct?
> A. That is, in fact, the quarantine policy. In other words, there's not two steps there. A quarantine policy is, in fact, checking the destination.
> Q. Okay. And if it says, block the packet, it will be prevented from the data transfer going there, right?
> A. That's right.
> Q. If it's not in there, and if there is a – it's able to go through to a permitted network or permitted resource, then the packet would be allowed to go through by the switch or the router. Isn't that right?
> A. That's right.

Tr. 2423:19-2424:15; *see* PTX-563 at 038414-415; PTX-1326 at 11.

29. Dr. Crovella even concedes that the '193 Patent requires a device to "block some communication between the two networks but allow other communication to flow." Tr. 2400:8-10. This is the exact functionality outlined by the asserted claims.

30. This described system, without the use of Stealthwatch, can identify exfiltrations and drop packets as a result. Therefore, Cisco's second theory of non-infringement is irrelevant to the Court's determination because the Catalyst 9000 Switches and ISR/ASR Routers operate to block packets based on the particular type of data transfer between networks as required by the claims. Cisco's technical documents, such as PTX-1294 and PTX-1326, demonstrate that Stealthwatch is not involved in this part of the infringing functionality. Accordingly, any evidence regarding Stealthwatch has no bearing on infringement for the '193 Patent.

ii. Centripetal has Proven Direct Infringement of the '806 Patent

31. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 9 and 17 of the '806 Patent by making, using, selling, offering for sale, and/or

importing the Catalyst 9000 Switch with DNA in the United States. See Findings of Fact, Section VI(A)(i)-(ii).

32. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 9 and 17 of the '806 Patent by making, using, selling, offering for sale, and/or importing the ISR/ASR Router with DNA in the United States. See Findings of Fact, Section VI(A)(i)-(ii).

33. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 9 and 17 of the '806 Patent by making, using, selling, offering for sale, and/or importing the Firewall with FMC in the United States. See Findings of Fact, Section VI(A)(iii).

34. Dr. Reddy advances three theories of non-infringement for the '806 Patent. He avers that the accused products: (1) do not cease processing of packets responsive to a signal; (2) do not cache the packets responsive to a signal; and (3) do not reprocess packets according to a second rule set. To prove that the products do not perform this functionality as required by the claims, Dr. Reddy relied on an animation produced for litigation that directly contradicts Cisco's employee testimony and Cisco's technical documents. Using this animation, Dr. Reddy opined that the Cisco products never cache or cease processing packets during a rule swap. Tr. 2610-2-8.

35. Turning to the first theory, Cisco employee, Peter Jones, testified that in the operation of packet processing, Cisco's the Catalyst 9000 Switch and ISR/ASR Router will store packets in a part of the UADP ASIC processor known as the Packet Buffer Complex ("PBC"). The PBC operates as a holding spot for the data in the payload of the packet while the header information is forwarded to another part of the processor for the application of rules. This operation in the Catalyst 9000 Switch and ISR/ASR Router is designed to maximize the speed

and efficiency of packet processing through software. Tr. 622:16-18. Dr. Mitzenmacher highlights that computer scientists use the term buffer and cache interchangeably as a word denoting the use of memory to hold packets for a short period of time. Tr. 628:7-25. Dr. Mitzenmacher referenced that a buffer is a "memory that holds something . . . [o]ften for future use." In reference to the Court's question about defining a cache, Dr. Mitzenmacher gave a similar definition of cache in the following exchange:

> Q. What's a cache?
> A. A cache is also often used, is used in the same way as a memory for holding things. They're very similar. And with a cache you don't typically or necessarily have an ordering associated with it. I mean, it can have an ordering, but it doesn't have to. But a cache is typically used as a memory that holds information that you expect to be using in the near future.

Tr. 836:17-23.

36. Martin Hughes, a Cisco Engineer, confirmed Dr. Mitzenmacher's opinion that a packet buffer is a cache. Mr. Hughes was asked:

> Q. When the router products receive a packet, do router products store the packet in the cache?
> A. All products have packet buffers where packets are stored before processing.

DTX-1650; see Tr. 628:3-25, 866:8-22.

37. The Packet Buffer Complex within the Catalyst 9000 Switch and ISR/ASR Router acts as a memory storage to hold packet information for further use, and therefore performs the same function of a cache, however, Cisco uses a different nomenclature, calling it a packet buffer. Tr. 836:17-23. Accordingly, in the course of packet processing, the Catalyst 9000 Switch and ISR/ASR Router store packets in a cache as required by the claims. *See* Findings of Fact, Section VI(A)(i) and (A)(ii)(f).

38. Cisco advances that the accused products do not cease processing of packets in response to a rule swap. Mr. Jones, a Cisco Engineer, testified contrary to this assertion. He

explained that the newly compiled rules are swapped for the old rules while no packets are being processed. Tr. 2572:10-20. Mr. Jones also stated that this reprogramming is done in response to a signal to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set. Tr. 2571:2-2573:9. Therefore, the Catalyst 9000 Switch and ISR/ASR Router operate using a "cease and cache" functionality where they cease packet processing and cache the packets to implement the newly compiled rule set. *See* Findings of Fact, Section VI(A)(i) and (A)(ii)(e-g).

39. With regard to both of these theories, Cisco argues that because this process is the normal processing functionality of the accused products, Cisco cannot in theory infringe the claims of the '806 Patent. However, Cisco has implemented this new rule swap functionality in conjunction with the normal processing functionality as outlined in the '806 Patent to greatly improve the security functionality of its products without dropping packets. The devices, in response to an initial signal, check whether packets are being processed. If so, the rule swap will not occur. If no packets are being processed and instead are held in the buffer, the processor signals to swap the rules. Once the swap is complete, another signal is made to indicate that the rules have been swamped and that the processing of packets with the new rules may begin. *See* Findings of Fact, Section VI(A)(i) and (A)(ii)(e-g).

40. Cisco argues that packets are not reprocessed by a second rule set. However, the claims do not require reprocessing of packets. The claims state that all that is required is for packets to be processed through a second rule set once the rules have been swapped. JTX-2. In other words, unprocessed packets must be processed by the second rule set after the swap – not processed a first time before the swap and processed again after the swap as Cisco suggests. Second, Cisco's non-infringement expert, Dr. Reddy, does not opine upon or even discuss the

egress portion of a packet's transmission through a switch, router or firewall. Mr. Jones and Cisco's technical documents confirm that the accused devices apply rules on both ingress into the device and on egress out of the device. Therefore, in their operation, the Catalyst 9000 Switch and ISR/ASR Router are configured to apply one set of rules on ingress while the very same packet would be subject to a second set of rules on egress within the same device. This process would meet the claim language of the '806 Patent to process packets with a first rule set and then in accordance with a second rule set even under Cisco's misreading of the claims. See Findings of Fact, Section VI(A)(i) and (A)(ii)(c-g).

41. The Firewall Product operates in a similar infringing manner. Cisco has not raised arguments specific to the Firewall, and its infringes for the same reason. See Findings of Fact, Section VI(A)(iii).

iii. Centripetal has Proven Direct Infringement of the '176 Patent

42. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 11 and 21 of the '176 Patent by making, using, selling, offering for sale and/or importing the Catalyst 9000 Switch with Stealthwatch in the United States. *See* Findings of Fact, Section VII(A)(i)-(iii).

43. Centripetal has proven by a preponderance of the evidence that Cisco literally infringes Claims 11 and 21 of the '176 Patent by making, using, selling, offering for sale and/or importing the ISR/ASR Router with Stealthwatch in the United States. *See* Findings of Fact, Section VII(A)(i)-(iii).

44. Dr. Almeroth advanced two non-infringement theories. Tr. 2239:17-2240:14. First, he claimed that none of the accused products correlate a plurality of transmitted packets with a plurality of received packets as required by the asserted claims of the '176 Patent. Tr.

2247:18-2248:4. Second, he claimed that none of the accused products generate and provision rules in response to those claimed correlations. Tr. 2247:18-2248:4.

45. Dr. Almeroth opined that Dr. Cole's infringement opinion relied on the use of logs provided by Cisco's proprietary logging technology, NetFlow, as the logs outlined by the claim language. Dr. Almeroth construed the claims to require identification and generation of logs out of the same network device on ingress and egress. Therefore, Dr. Almeroth avers that the Cisco system cannot infringe, because in his opinion, the Catalyst 9000 Switch and ISR/ASR Router do not generate NetFlow on both ingress into a device and egress out of one network device. Tr. 2249:4-18. Cisco's technical documents refute Dr. Almeroth's conclusion.

46. PTX-1060, a Cisco technical document dated December of 2017, shows that the Catalyst 9000 Switch has the ability to export NetFlow on ingress and egress. Tr. 986:18-987:1; PTX-1060 at 023 (showing that the Catalyst 9400 switch is capable of supporting 384,000 NetFlow entries – 192,000 on ingress and 192,000 on egress). Dr. Almeroth, on cross-examination, even admitted that the Catalyst 9000 Switch and ISR/ASR Router can be configured to export ingress and egress NetFlow.

> Q. Isn't it correct, Dr. Almeroth, that this Cisco document says right here that MPLS Egress and NetFlow Accounting feature can be used -- being use to capture ingress and egress flow statistics for router B, one device. Is that correct?
>
> A. That's what it says. But my last answer was qualified for Stealthwatch. This document, at least what you're pointing me to here, does not mention Stealthwatch. And that was really my whole point: That you can certainly configure NetFlow ingress and egress, but when you get to troubleshooting Stealthwatch, it's considered an error within Stealthwatch.

Tr. 2286:10-19.

47. In this exchange, Dr. Almeroth confirms that NetFlow can be configured on ingress and egress but shifts the crux of his non-infringement opinion to the fact that

Stealthwatch produces an error based on producing both types of NetFlow. To support that claim, Dr. Almeroth relied solely on source code from the 6.5.4 version of Stealthwatch that operated without enhanced NetFlow or the integration of Cognitive Threat Analytics (CTA). Tr. 2287:1-19; see DTX-1616 (showing source code from a previous 6.5.4 version of Stealthwatch that is not accused by Centripetal). He cites to no technical document that confirms that the accused/current version of Stealthwatch produces an error when exporting both ingress and egress NetFlow. In fact, the technical release notes for CTA, which was incorporated into Stealthwatch in 2018, support that CTA produced the ability for the correlation of NetFlow telemetry. PTX-1009 at 009.

48. Dr. Cole, in his infringement opinion on the "identify and generate" elements, proved that one network device generate logs on a packet's ingress and egress out of the device. Moreover, in any case, the Asserted Claims are not limited to analyzing ingress and egress out of one device. See Findings of Fact, Section VII(A)(i) and (A)(ii)(b-c).

49. Based on the testimony and technical documents, the Catalyst 9000 Switch and ISR/ASR Router do identify and generate logs on ingress and egress. However, a look at the specification of the '176 Patent informs the Court that this is not the only application that would infringe the asserted claims. These claim elements would also be met if there was identification, generation and correlation of logs from two different network devices on either ingress or egress. JTX-3 at 8:46-63 of the specification highlights that:

> At step **16**, packet correlator **128** may utilize log(s) **142** to correlate the packets transmitted by network device(s) **122** with the packets received by network device(s) **122**. For example, packet correlator **128** may compare data in entry **306** with data in entry **312** (e.g., network-layer information, transport-layer information, application-layer information, or environmental variable(s)) to correlate **P1'** with **P1** (e.g., by determining that a portion of the data in entry **306** corresponds with data in entry **312**). Similarly, packet correlator **128** may compare data in entry **308** with data in entry **314** to correlate **P2'** with **P2**, packet correlator **128** may compare data in entry **310** with data in entry **316** to correlate **P3'** with **P3**, packet correlator **128** may compare data in entry **318** with data in entry **324** to correlate **P4'** with **P4**, packet correlator **128** may compare data in entry **320** with data in entry **326** to correlate **P5'** with **P5**, and packet correlator **128** may compare data in entry **322** with data in entry **328** to correlate **P6'** with **P6**.

JTX-3 at 8:46-63.

50. Additionally, it is undisputed that bidirectional flows are captured, which requires data to be collected from both directions. As such, bidirectional Netflow is captured (packets both sent and received between hosts), as discussed in the Cisco document PTX-569 at 282, which states that "[a]ny interface that is missing inbound or outbound traffic is not configured properly … [and in the example] all are reporting inbound and outbound traffic".

51. This section of the specification indicates that the network device that generates the correlated logs may be plural as well as singular. Additionally, this section is showing the correlation may occur between data entries that were processed through two different network devices. *Compare* JTX-3, 8:46-63 *with* JTX-3, Fig. 3. Dr. Almeroth, on cross-examination, confirms that the use of "a network device" in the claim language may mean more than one network device:

> Q. And then you said this had to be a single network device, correct?
> A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.

> Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?
> A. That's my understanding.
> Q. So this could be more than one network device, correct?
> A. It could be.

Tr. 2278:11-20; *see also Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342-43 (Fed. Cir. 2008) (when drafting a patent claim, "a" means "one or more").

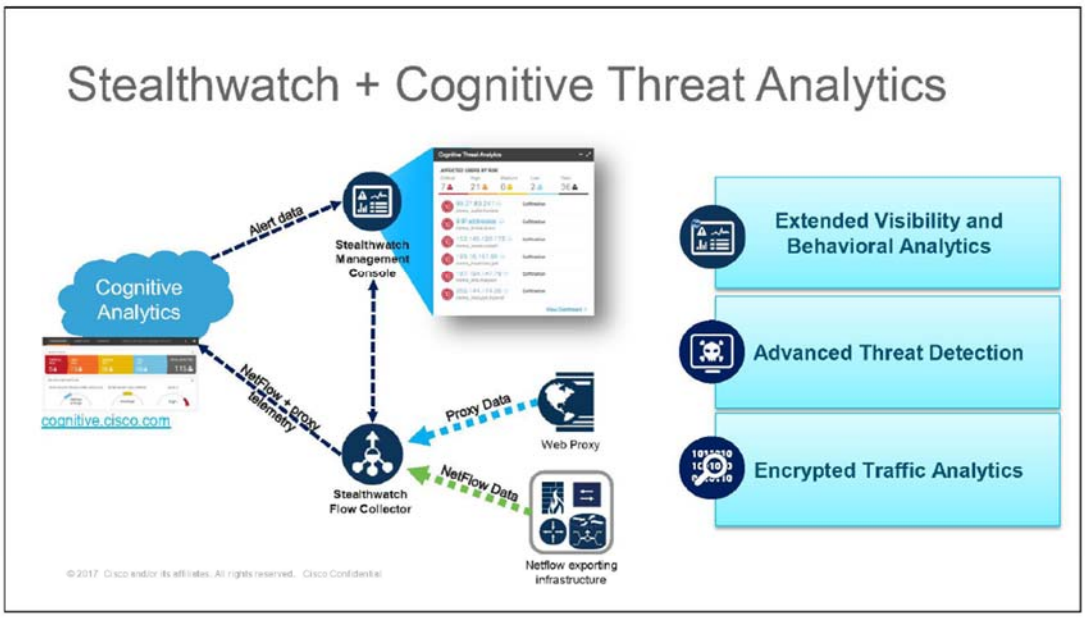
52. Therefore, even if Dr. Almeroth's conclusion that the Catalyst 9000 Switch and ISR/ASR Router do not process ingress and egress out of the same device is accepted, there is still infringement on the basis that the Cisco system correlates bidirectional logs between multiple devices within the network on either ingress or egress. *See* Findings of Fact, Section VII(A)(i) and (A)(ii)(b-c).

53. Moreover, Dr. Almeroth states that the accused system does not generate and provision rules in response to correlation performed by Stealthwatch and CTA. Dr. Almeroth admits that Stealthwatch with CTA performs correlations, just not correlations required by the claim language. In explaining the diagram of PTX-1065, Dr. Almeroth opined:

> Q. Can you explain what's going on here, Dr. Almeroth?
> A. Yes. What's being shown here, if you start in the bottom, it shows two different sources of information that ultimately get correlated. There's proxy data and there's NetFlow data. And when Dr. Cole testified, he represented that that NetFlow data included ingress and egress records from the same device, which was actually not the case, as the evidence and the correct operation of the devices show. And then from there, his analysis principally turned on the fact that these documents describe correlation. They absolutely use the word correlation, but it's not the correlation of the type required by the claims. And the example that's shown in this particular figure and what's described in the text below is that you're correlating NetFlow data, which is not the NetFlow data required by the claim for the reasons I've given, with other data. In this case, proxy data. And so even though these documents use the word correlate, what they're correlating is not the kind of correlation that's required by the claims.
>
> Q. Okay. And if we look, Mr. Simons, at the text below?
> BY MR. JAMESON:

Q. And I don't want to go through all of this, but is the same point made in the text below with respect to the comments you made, about the diagram?
A. Yes. It's absolutely the case that Stealthwatch correlates I think what we've referred to as threat intelligence with NetFlow records. But what it is not comparing, what it is not correlating is it's not correlating the NetFlow records to themselves as required by the elements of the claims, because it tries to block or double count those NetFlow records. And so all of this evidence that Dr. Cole relied on that uses the word correlate, over and over again it describes correlation of threat intelligence with NetFlow data, which is not what the claim requires and also is not what the '176 patent is about.

Tr. 2256:3-2257:10.



Stealthwatch integrates with Cognitive Analytics ("CA" – aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

PTX-1065 at 0005.

54. As shown, Dr. Almeroth agrees that Stealthwatch correlates NetFlow and Syslog information. PTX-202 states that Stealthwatch "correlates local traffic models with global threat behaviors to give you rich threat context around network traffic . . . and applies encrypted traffic analytics to enhance NetFlow analysis." PTX-202 at 242. Therefore, Stealthwatch uses the

NetFlow information within the network to correlate those records to each other and global threat indicators. However, this is not Stealthwatch's only use of correlation. In order to make use of behavioral analytics, Stealthwatch correlates NetFlow that passes through network devices to create a baseline of normal types of traffic that would pass through the network. This correlation occurs between both NetFlow and other logs provided to Stealthwatch in the form of WebFlow telemetry through the use of Syslog. Therefore, along with matching threats to global threat indicators, Stealthwatch can also detect threats based on abnormal activity that occurs within the network. For example, a large amount of data being transported throughout the network at a time where an office is closed or not conducting business would send up an alert that something malicious may be afoot. See Findings of Fact, Section VII(A)(i) and (A)(ii)(b-c).

55. Cisco's technical guide for configuring Netflow and Stealthwatch, PTX-569, illustrates how Stealthwatch "[c]reates a baseline of normal behavior" and "correlates threat behaviors seen in the local environment with those seen globally."

Doc type
Cisco public

CISCO

Stealthwatch Enterprise also integrates with a cloud based multi-stage machine learning analytics engine, that correlates threat behaviors seen in the local environment with those seen globally. It employs a funnel of analytical techniques to detect advanced threats.

Figure 3: Detect anomalies and threats

For more information about the Stealthwatch components and architecture, please refer to the Stealthwatch Enterprise Data Sheet.

PTX-569 at 272.

56. This process would require Stealthwatch to correlate NetFlow within the network between multiple devices in order to recognize normal traffic patterns within the network.

57. Accordingly, it is axiomatic that Stealthwatch could then provision rules to stop threats detected based on internal network NetFlow correlation with or without global threat indicators. PTX-595 at 179.

58. Therefore, Stealthwatch performs the exact type of correlation and provisioning of rules in response to correlations required by the '176 Patent.

B. Infringement under Doctrine of Equivalents

59. "[A] product or process that does not literally infringe upon the express terms of a patent claim may nonetheless be found to infringe if there is 'equivalence' between the elements of the accused product or process and the claimed elements of the patented invention." *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 21 (1997). Infringement under the doctrine of equivalents exists when each limitation recited in the asserted claim, or its equivalent, is found in the accused product. *Abraxis Bioscience, Inc. v. Mayne Pharma (USA) Inc.*, 467 F.3d 1370, 1379 (Fed. Cir. 2006) (internal quotation omitted). An equivalent performs substantially the same function as the claimed limitation in substantially the same way, to achieve substantially the same result. *Id.*; *see also Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 608 (1950).

60. A plaintiff is entitled to the doctrine of equivalents when it either (1) made no amendments such that prosecution history estoppel does not apply, or (2) made no clear disavowal and surrender of subject matter because the amendment was tangential to the equivalent at issue. *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 722, 740-41 (2002). Further, even if prosecution history estoppel applies, it "does not completely bar the benefit of the doctrine of equivalents from all litigation related to the amended claim." *Intervet*

Inc. v. Merial Ltd., 617 F.3d 1282, 1291 (Fed. Cir. 2010). "The scope of the estoppel must fit the nature of the narrowing amendment." *Id.* "A district court must look to the specifics of the amendment and the rejection that provoked the amendment to determine whether estoppel precludes the particular doctrine of equivalents argument being made." *Id.*

61. Centripetal is entitled to the doctrine of equivalents for the Asserted Claims of the '193 Patent because it made no amendments to those claims during prosecution. Thus, the doctrine of prosecution history estoppel is inapplicable to the claims.

62. Centripetal is entitled to the doctrine of equivalents for the Asserted Claims of the '806 Patent because it "made no clear disavowal and surrender of subject matter" by amendment during prosecution. *See Festo Corp.*, 535 U.S. at 740-41. Thus, there is no prosecution history estoppel against Centripetal.

63. Applying this Court's claim construction and based the facts and expert evidence presented at trial, Centripetal has proven by a preponderance of the evidence that the Accused Products infringe the Asserted Claims of the '193 and '806 Patents under the doctrine of equivalents.

64. Centripetal has proven by a preponderance of the evidence that Cisco's Catalyst 9000 Switch infringes Claims 18 and 19 of the '193 Patent under the doctrine of equivalents. See Findings of Fact, Section V(A)(iii).

65. Centripetal has proven by a preponderance of the evidence that Cisco's ISR/ASR Router infringes Claims 18 and 19 of the '193 Patent under the doctrine of equivalents. See Findings of Fact, Section V(A)(iii).

66. Centripetal has proven by a preponderance of the evidence that Cisco's Catalyst 9000 Switch with DNA infringes Claims 9 and 17 of the '806 Patent under the doctrine of equivalents. See Findings of Fact, Section VI(A)(iv).

67. Centripetal has proven by a preponderance of the evidence that Cisco's ISR/ASR Router with DNA infringes Claims 9 and 17 of the '806 Patent under the doctrine of equivalents. See Findings of Fact, Section VI(A)(iv).

68. Centripetal has proven by a preponderance of the evidence that Cisco's Firewall with FMC infringes Claims 9 and 17 of the '806 Patent under the doctrine of equivalents. See Findings of Fact, Section VI(A)(iv).

C. Induced Infringement

69. Cisco has and continues to actively induce its customers to infringe the Asserted Patents because Cisco had knowledge of these patents and knew or willfully blinded itself to the fact that its actions were aiding and abetting direct infringement. 35 U.S.C. § 271(b). Induced infringement exists when a defendant knows of the existence of a patent and knows that its actions will induce actual infringement by another. *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 766 (2011). It is sufficient that the defendant was willfully blind to the induced infringement, where "(1) [t]he defendant must subjectively believe that there is a high probability that a fact exists and (2) the defendant must take deliberate actions to avoid learning of that fact." *Id.* at 769. Notably, a belief that a patent is invalid is not a defense against induced infringement. *Commil USA, LLC v. Cisco Sys., Inc.*, 575 U.S. 632, 636 (2015). To induce infringement the accused infringer must have taken "affirmative steps" to bring about direct infringement. *Global-Tech Appliances, Inc. v. SEB S.A.,* 563 U.S. 754, 760 (2011).

70. The record is replete with Cisco taking affirmative steps to cause the infringement of its customers, including through marketing materials, white papers, and guides showing that

the Accused Products are designed for customers to use for their infringing functionalities, and that Cisco deliberately encourages users and instructs users on how to infringe. *See* Findings of Fact, Section VIII(A) (citing, *inter alia*, PTX-1289 (Firepower configuration guide), PTX-1135 (press release touting built-in security unique to Cisco network devices with DNA), PTX-197 (showing benefits of Firewalls with FMC), PTX-276 (marketing Stealthwatch as part of Switches and Routers), PTX-1507 (benefits of upgrading to ISR Routers)).

71. Customer use of the Accused Products to infringe constitutes acts of direct infringement under 35 U.S.C. § 271(a). The evidence supports that Cisco's customers infringe, including the evidence that Cisco repeatedly touted the success and efficacy of the infringing functionalities and that Cisco enjoyed increased revenues after releasing the infringing functionalities.

72. Cisco does not dispute that its customers use the infringing functionalities of the Accused Products. Such use is direct infringement under 35 U.S.C. § 271(a).

73. Cisco knew of the '806 Patent before the filing of Centripetal's Complaint, as early as February 2016. *See* Findings of Fact, Sections VIII(J), IX(A). Despite knowing of the patent and knowing that it was deploying Centripetal's patented technology (and thus knowing of its infringement, *see* Findings of Fact, Sections II(C)-(D), VIII(J), and IX(A)), Cisco released the Catalyst 9000 Switch with DNA, ISR/ASR Router with DNA, and Firewall with FMC.

74. Cisco received notice of the '806, '176, and '193 Patents on February 13, 2018 with the filing of the Complaint. *See* Findings of Fact, Section VIII(J).

75. Despite knowing about the Asserted Patents and knowing that its customers' use of the Accused Products was infringing as of the dates of the complaints, Cisco has induced and continues to induce such infringement.

76. Applying this Court's claim construction and based on the facts and expert evidence presented at trial, Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of the Asserted Claims of the Asserted Patents with the Accused Products.

77. Centripetal has proven by a preponderance of the evidence that Cisco's customers directly infringe the Asserted Claims of the Asserted Patents because they use the infringing functionalities of the Accused Products.

78. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 18 and 19 of the '193 Patent with Cisco's Catalyst 9000 Switch.

79. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 18 and 19 of the '193 Patent with Cisco's ISR/ASR Router.

80. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 9 and 17 of the '806 Patent with Cisco's Catalyst 9000 Switch with DNA.

81. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 9 and 17 of the '806 Patent with Cisco's ISR/ASR Router with DNA.

82. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 9 and 17 of the '806 Patent with Cisco's Firewall with FMC.

83. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 11 and 21 of the '176 Patent with Cisco's Catalyst 9000 Switch with Stealthwatch.

84. Centripetal has proven by a preponderance of the evidence that Cisco induces its customers' infringement of Claims 11 and 21 of the '176 Patent with Cisco's ISR/ASR Router with Stealthwatch.

III. VALIDITY

A. Presumption of Validity

85. The Asserted Patents are presumed valid. 35 U.S.C. § 282(a). Each claim is presumed valid independent of the validity of any other claim, and the burden of demonstrating invalidity rests with the party asserting invalidity. *Id.*

B. Standard for Institution of IPRs and Estoppel

86. The PTAB may institute an *inter partes* review proceeding if it determines that the information presented in the petition seeking review and in any patent owner's response shows "a reasonable likelihood that the petitioner would prevail with respect to at least one of the claims challenged in the petition." 35 U.S.C. § 314.

87. To show invalidity in an instituted *inter partes* review proceeding, the petitioner must demonstrate unpatentability by a preponderance of the evidence. 35 U.S.C. § 316(e).

88. Cisco is estopped from presenting any alleged ground for invalidity that it raised or reasonably could have raised in Cisco's *inter partes* review proceedings that resulted in a Final Written Decision. 35 U.S.C. § 315(e)(2). Grounds that the petitioner "reasonably could have raised" are grounds that "a skilled searcher conducting a diligent search reasonably could have been expected to discover." *Trustees of Columbia Univ. in the City of New York v. Symantec Corp.*, 390 F. Supp. 3d 665, 677-78 (E.D. Va. 2019) (holding defendant was statutorily estopped from relying on those grounds of invalidity that it previously identified in its invalidity contentions in patent infringement suit, but that software company chose not to assert in its intervening inter partes review petitions); *Wi-LAN Inc. v. LG Elecs., Inc.*, 421 F. Supp. 3d 911,

926 (S.D. Cal. 2019) (enforcing estoppel on grounds raised in IPRs and further estopping the use of alleged prior art which was cited within references which the challenging party had raised in IPRs); *Ironburg Inventions Ltd. v. Valve Corp.*, 418 F. Supp. 3d 622, 631 (W.D. Wash. 2019) (enforcing estoppel on grounds raised in IPRs and further estopping the use of alleged prior art cited in other contemporaneous IPRs or cited on face of patent because they "reasonably could have been raised"). Even if the exact reference is not raised at trial, it is still harder to meet the clear and convincing burden at trial when the references asserted rely on substantially the same arguments as those raised in the IPR. *Sciele Pharma Inc. v. Lupin Ltd.*, 684 F.3d 1253, 1260 (Fed. Cir. 2012) ("[I]t may be harder to meet the clear and convincing burden when the invalidity contention is based upon the same argument on the same reference that the PTO already considered.").

C. Standard for Validity in District Court Litigation

89. In contrast to *inter partes* review proceedings, in district court, the party challenging the validity of a patent must prove its case by clear and convincing evidence. *Microsoft Corp. v. I4I Ltd. P'ship*, 564 U.S. 91, 95 (2011). "Clear and convincing evidence" is generally described as evidence that "place[s] in the ultimate factfinder an abiding conviction that the truth of its factual contentions are highly probable." *Colorado v. New Mexico,* 467 U.S. 310, 316(1984) (internal quotations omitted). The burden of proof never shifts to the patentee to prove validity. *Hybritech Inc. v. Monoclonal Antibodies, Inc.,* 802 F.2d 1367, 1375 (Fed.Cir.1986). However, whether the challenger has met its burden by clear and convincing evidence is determined by considering the totality of the evidence, including any rebuttal evidence presented by the patentee. *Stratoflex, Inc. v. Aeroquip Corp.,* 713 F.2d 1530, 1534 (Fed.Cir.1983).

90. Cisco failed to meet the standard to institute *inter partes* review on multiple alleged grounds for invalidity, which ostensibly were Cisco's best grounds for the purported invalidity of Centripetal's patents. Cisco now raises the same grounds on which it failed to obtain institution in district court. However, the PTAB already determined that the grounds on which it denied institution of *inter partes* review did not demonstrate "a reasonable likelihood that the petitioner would prevail with respect to at least one of the claims challenged in the petition." 35 U.S.C. § 314. If Cisco's prior art asserted in a petition to institute *inter partes* review failed to show "a reasonable likelihood" of success with respect to at least one claim, it cannot possibly meet the clear and convincing evidence standard required in district court litigation.

91. The *inter partes* review process incentivizes patent challengers to put forth their best allegations regarding validity to the PTAB, because the PTAB's Final Written Decisions have a preclusive effect on what the patent challenger can assert in district court. As Cisco presented its best prior art in its *inter partes* petition under a lower burden of proof, Cisco cannot meet its burden of proving by clear and convincing evidence of invalidity with Cisco's left over prior art used in this District Court proceeding. 35 U.S.C. § 315(e)(2) (estopping both grounds raised in IPR and grounds that reasonably could have been raised). To the extent that Cisco later invented new allegations for invalidity which it did not know of when it filed its numerous IPRs, and which "a diligent search" by "a skilled researcher" could not find to assert in IPRs, such "afterthought" arguments cannot possibly meet the clear and convincing evidence standard to rebut the presumption of validity.

92. Cisco failed to meet its burden of proving invalidity of any claim of the Asserted Patents by clear and convincing evidence. The Asserted Claims of the Asserted Patents are valid.

93. With respect to the '193 Patent, Cisco failed to offer any evidence that the old quarantine technology was the same as the new quarantine functionality accused of infringement. Moreover, Cisco failed to offer any evidence as to whether packet-filtering rules, a first operator, or a second operator were present in the prior art which are requirements of the asserted claims in the '193 Patent.

94. With respect to the '806 Patent, Cisco failed to offer any evidence that the alleged prior art contained the same functionality accused of infringement because the alleged prior art would not swap rules. Instead, in the alleged prior art, rules would overlap which would cause packets to drop. Moreover, Cisco failed to offer any evidence that the alleged prior art received a first rule set, received a second rule set, preprocessed a first rule set, or preprocessed a second rule set which are requirements of the Asserted Claims in the '806 Patent.

95. With respect to the '176 Patent, Cisco failed to offer any evidence that the alleged prior art contained the same functionality accused of infringement because the alleged prior art, namely old Steathwatch, did not contain Cognitive Threat Analytics. Moreover, Cisco failed to offer any evidence that the alleged prior art performed correlation and generate or provision rules which are requirements of the asserted claims in the '176 Patent.

D. Alleged Anticipation under 35 U.S.C. § 102(a) and § 102(b)

96. The '193 Patent and '806 Patent are subject to the pre-AIA Patent Act. Under pre-AIA section 102(a), to prove anticipation, Cisco must prove by clear and convincing evidence that the invention of the Asserted Patent "was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention

thereof by the applicant for patent." 35 U.S.C. § 102(a) (pre-AIA). Under section 102(b), Cisco must prove by clear and convincing evidence that the invention of the Asserted Patent "was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States." 35 U.S.C. § 102(b) (pre-AIA).

97. The '176 Patent is subject to the post-AIA Patent Act. Under AIA section 102(a), to prove anticipation, Cisco must prove by clear and convincing evidence that either "(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention; or (2) the claimed invention was described in a patent … or in an application for patent published or deemed published … in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention." 35 U.S.C. § 102(a) (AIA).

98. An alleged prior art reference under section 102 (pre-AIA or AIA) only invalidates "if each and every limitation is found either expressly or inherently in a ***single*** prior art reference. The elements must be arranged or combined in the same way as in the claim, but the reference need not satisfy an *ipsissimis verbis* test. Also, the reference must enable one of ordinary skill in the art to make the invention without undue experimentation." *Whitserve, LLC v. Comput. Packages, Inc.*, 694 F.3d 10, 21 (Fed. Cir. 2012) (internal citations and quotation marks omitted) (emphasis added).

99. For a claim element to be inherently found in a single reference, Cisco must prove by clear and convincing evidence that the missing limitation is "necessarily present" in the alleged prior art reference. *Cont'l Can Co. USA v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir.

1991). It is insufficient to show that the limitation "may" exist in the alleged prior art reference. *Id.* at 1269 (quoting *In re Oelrich,* 666 F.2d 578, 581 (CCPA 1981)).

100. "When more than one reference is required to establish unpatentability of the claimed invention anticipation under § 102 cannot be found, and validity is determined in terms of § 103." *Cont'l Can Co. USA*, 948 F.2d at 1267. As a matter of law, Cisco cannot assert multiple references in combination with one another as anticipatory.

101. Cisco failed to meet its burden of proving by clear and convincing evidence that any limitation recited in any claim of the Asserted Patents is explicitly or inherently present in the asserted alleged prior art.

E. Alleged Obviousness under 35 U.S.C. § 103

102. Under section 103 of the Patent Act, an invention is obvious "if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." 35 U.S.C. §103 (AIA).[2] Cisco must demonstrate by clear and convincing evidence that a patent claim is invalid by showing that the claimed invention would have been obvious to persons having ordinary skill in the art at the priority date of the Asserted Patents. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 420-21 (2007).

103. To prove obviousness, Cisco must first demonstrate by clear and convincing evidence that the alleged asserted references satisfy the requirements to qualify as prior, as set forth in section 102. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568 (Fed. Cir. 1987).

[2] The pre-America Invents Act ("AIA") version of Section 103 of the Patent Act and the post-AIA version are substantially the same with respect to the standard for proving obviousness.

104. Then, Cisco must prove four separate elements:

(1) determine the scope and content of the alleged asserted prior art;

(2) determine the differences between the claim invention and the alleged asserted prior art;

(3) determine and define the person of ordinary skill in the art; and

(4) determine whether the person of ordinary skill in the art would find the differences between the claim and the alleged prior art obvious, taking into account secondary considerations.

Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 17-18 (1966).

105. Notably, "a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418.

106. In addition, for each alleged combination of references, Cisco must demonstrate "by clear and convincing evidence that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so." *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1361 (Fed.Cir.2007).

107. Cisco failed to prove by clear and convincing evidence that any single alleged prior art reference or combination of alleged prior art references render the invention of any Asserted Patent obvious.

108. Cisco also failed to prove by clear and convincing evidence that a person of skill in the art would be motivated to combine any alleged prior art references.

109. Cisco failed to even define a person of skill in the art, as required under the *Graham* factors. *Graham*, 383 U.S. at 17-18. This failure undermines any alleged response by Cisco to these factors.

110. As part of the fourth step, courts must consider secondary considerations, also called objective indicia, of non-obviousness. *Id.*; *Leo Pharm. Prod., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013); *Transocean Offshore Deepwater Drilling, Inc.*, 699 F.3d at 1349. Courts must consider secondary considerations in order to counter hindsight bias. *Graham*, 383 U.S. at 36. "[E]vidence of secondary considerations may often be the most probative and cogent evidence in the record. It may often establish that an invention appearing to have been obvious in light of the prior art was not. This objective evidence must be considered as part of all the evidence, not just when the decisionmaker remains in doubt after reviewing the art." *Transocean Offshore Deepwater Drilling*, 699 F.3d at 1349 (internal citations and quotation marks omitted). A patent challenger may not rebut the presumption of nexus with argument alone. *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1329 (Fed. Cir. 2016).

111. The secondary considerations of non-obviousness are:

(1) commercial success;

(2) industry praise or unexpected results;

(3) the failure of others;

(4) copying by others;

(5) industry skepticism;

(6) licensing; and

(7) whether the invention provides a solution to a long-felt but unsolved need.

Graham, 383 U.S. at 17-18; *Transocean Offshore Deepwater Drilling*, 699 F.3d at 1349-54.

112. Based on all the facts and expert evidence presented at trial, the secondary considerations in this case support a finding of non-obviousness. Centripetal established that the secondary considerations were met, which Cisco did not rebut with any evidence of its own, only conclusory statements. See Findings of Fact, Sections V(B), VI(B), and VII(B).

113. Dr. Striegel proved that the objective indicia of non-obviousness for the '193 Patent, including recognition of the problem, long-felt need in the industry, failure of others, praise by others, industry recognition, copying, and licensing. Cisco did not rebut this analysis. See Findings of Fact, Sections V(B).

114. Dr. Striegel established traditional solutions suffered because they could not handle the increasing volume of data on networks, nor the speed at which attacks changed and that the '193 Patent addressed this because it proactively brought together threat intelligence to combat threats. The '193 Patent's invention provided a solution to the problem of exfiltration that had yet to be solved prior to Centripetal's invention. *See* Findings of Fact, Sections V(B).

115. There was a failure of others in the industry to provide proactive network protection such as the '193 Patent invention that could scale to larger networks and address emerging threats efficiently. The existing solutions were reactive, inflexible and non-scalable and many lacked automation and the inability to use threat intelligence in a meaningful way to live network traffic and use threat intelligence into actionable insight into traffic on the network. See Findings of Fact, Sections V(B).

116. Cisco's copying of the invention of the '193 Patent is a secondary consideration of non-obviousness. See Findings of Fact, Sections V(B).

117. Dr. Striegel established that there was evidence of licensing the '193 Patent through the Keysight License. See Findings of Fact, Sections V(B).

118. Dr. Striegel proved the objective indicia of non-obviousness for the '806 Patent, including recognition of the problem, long-felt need in the industry, failure of others, praise by others, industry recognition, copying, and licensing. See Findings of Fact, Sections VI(B).

119. Dr. Striegel proved that traditional solutions were unable to address the problem of performing policy updates without affecting device performance. The '806 Patent solved the problem of rapidly swapping massively scaled cyberthreat intelligence policies to live Internet traffic without dropping packets or sacrificing security. The existing solutions were reactive, inflexible and non-scalable and lacked automation and the inability to use threat intelligence in a meaningful way to live network traffic and use threat intelligence into actionable insight into traffic on the network, such that there was a failure of others in the industry to provide protective network protection like the '806 Patent. *See* Findings of Fact, Sections VI(B).

120. Dr. Striegel established industry praise for the '806 Patent because Centripetal was identified as a "Cool Vendor" in PTX-1122 at 019854, which described aspects of the claims. There was industry recognition and praise for the invention of the asserted claims of the '806 Patent. Gartner recognized Centripetal's patented technology as "unique" and the importance of it being able to "load large indicator datasets," a problem specifically addressed by the '806 Patent. *See* Findings of Fact, Sections VI(B).

121. Cisco copied the invention of the '806 Patent. See Findings of Fact, Sections VI(B).

122. Dr. Striegel established that there was evidence of licensing the '806 Patent through the Keysight License. See Findings of Fact, Sections VI(B).

123. Dr. Striegel established the objective indicia of non-obviousness for the '176 Patent, including recognition of the problem, long-felt need in the industry, failure of others,

praise by others, industry recognition, copying, and licensing. See Findings of Fact, Sections VII(B).

124. Dr. Striegel established the problem the '176 Patent addressed when he discussed PTX-1113, an Office of Naval Research document that he described as showing a drastically increasing threat space, with attacks increasing in sophistication and the number of devices available to attack increasing. Dr. Striegel further testified how traditional solutions suffered because they could not handle the increasing volume of data on networks, nor the speed at which attacks changed, which the '176 Patent addressed this because it proactively brought together threat intelligence to combat threats. *See* Findings of Fact, Sections VI(B).

125. Dr. Striegel established the long-felt need for the '176 Patent using PTX-1112 at 013864-65, because it speaks to the need of those to go resolve the problem addressed by the '176 Patent, and specifically called out correlation. The evidence showed long-felt need for the invention of the '176 Patent asserted claims. *See* Findings of Fact, Sections VI(B).

126. Cisco copied the invention of the '176 Patent. *See* Findings of Fact, Section IX(A). Dr. Striegel established that there was evidence of copying the '176 Patent. Tr. 3223:10-3224:3.

127. Dr. Striegel established that there was evidence of licensing the '176 Patent through the Keysight License. *See* Findings of Fact, Sections VI(B).

F. Any Alleged Prior Art Must Be Publicly Accessible

128. Cisco failed to prove by clear and convincing evidence that certain references it alleges are prior art were patented, described in a printed publication, or in public use, on sale, or otherwise available to the public" before the relevant date. *See* 35 U.S.C. § 102(a)(1).

129. Cisco must prove that each alleged reference was publicly accessible in order to demonstrate that it constitutes a printed publication. *Acceleration Bay, LLC v. Activision*

Blizzard Inc., 908 F.3d 765, 772 (Fed. Cir. 2018) (citations and internal quotations omitted). A reference is considered publicly accessible only if it was "disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Id.* Cisco bears the burden to demonstrate public accessibility during the relevant time period. *Id.*; *In re Lister*, 583 F.3d 1307, 1316 (Fed. Cir. 2009).

130. Cisco must prove by clear and convincing evidence that each alleged "reference" product or system was publicly known or used in the United States during the relevant time period before the priority date of the Asserted Patents. 35 U.S.C. § 102; *see Hilgraeve Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 973-977 (E.D. Mich. 2003) (granting summary judgment that software was not publicly known because there was no evidence that it was sold or used in the United States).

131. Cisco failed to prove that Cisco's alleged prior art Catalyst 6500 series Supervisor Engine 2T (e.g., Sup 2T models VS-S2T-10G and VS-S2T-10G-XL) running IOS Release 12.2(50)SY and Cisco Prime Network Control System ("Catalyst 6500") was known or used by others in the United States before the invention date of the '806 Patent, under 35 U.S.C. § 102(a) (pre-AIA).

132. Cisco failed to prove that Cisco's alleged prior art Catalyst 6500 was in public use or on sale in the United States before the invention date of the '806 Patent, under 35 U.S.C. § 102(b) (pre-AIA).

133. Cisco failed to prove that the non-patent reference(s) Cisco relied on for its alleged prior art Catalyst 6500 was a printed publication before the invention date of the '806 Patent, under 35 U.S.C. § 102(b) (pre-AIA).

134. Cisco failed to prove that Cisco's alleged prior art CTDS was known or used by others in the United States before the invention date of the '193 Patent, under 35 U.S.C. § 102(a) (pre-AIA).

135. Cisco failed to prove that Cisco's alleged prior art CTDS was in public use or on sale in the United States before the invention date of the '193 Patent, under 35 U.S.C. § 102(b) (pre-AIA).

136. Cisco failed to prove that the non-patent reference(s) Cisco relied on for its alleged prior art CTDS was a printed publication before the invention date of the '193 Patent, under 35 U.S.C. § 102(b) (pre-AIA).

137. Cisco failed to prove that Cisco's alleged prior art system of (1) a prior art Cisco router or Catalyst switch and (2) Lancope Stealthwatch Enterprise version 6.5.4 were in public use, on sale, or otherwise available to the public before the invention date of the '176 Patent under 35 U.S.C. § 102(a)(1) (AIA).

138. Cisco failed to prove that the non-patent reference(s) Cisco relied on for its alleged prior art system of (1) a prior art Cisco router or Catalyst switch and (2) Lancope Stealthwatch Enterprise version 6.5.4 was a printed publication before the invention date of the '176 Patent under 35 U.S.C. § 102(a)(1) (AIA).

139. With regard to the '193 Patent, Dr. Crovella's discussion of quarantining was very different than the quarantining functionality that is present in the switches and routers accused of infringement.

G. Written Description

140. A patent requires a specification, which "shall contain a written description of the invention …" 35 U.S.C. § 112(a).[3] To prove an alleged lack of adequate written description, the party challenging validity must prove by clear and convincing evidence that the written description fails to adequately describe the claimed invention. *Allergan, Inc. v. Sandoz Inc.*, 796 F.3d 1293, 1309 (Fed. Cir. 2015). The specification need only "convey with reasonable clarity to those skilled in the art that, as of the filing date sought, [the inventor] was in possession of the invention,' and demonstrate that by disclosure in the specification of the patent." *Carnegie Mellon Univ. v. Hoffmann-La Roche Inc.*, 541 F.3d 1115, 1122 (Fed. Cir. 2008) (citation omitted) (quoting *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991)); *Moba, B.V. v. Diamond Automation, Inc.*, 325 F.3d 1306, 1321 (Fed. Cir. 2003). The specification need not exhaustively or exactly describe the subject matter claimed, as long as it otherwise identifies to one of ordinary skill in the art that the inventor invented what is claimed. *Union Oil Co. of California v. Atl. Richfield Co.*, 208 F.3d 989, 997 (Fed. Cir. 2000).

141. Cisco failed to prove by clear and convincing evidence that any of the Asserted Patents lack sufficient written description of the disclosed inventions. The Asserted Patents satisfy the written description requirement of Section 112 of the Patent Act.

142. The only terms that were specifically identified by Cisco, that of "correlate" and "responsive to correlating," were shown to be described and present in the specification of the '176 Patent when it was filed. See Findings of Fact, Section VII(B).

[3] The pre-America Invents Act ("AIA") version of Section 112 of the Patent Act and the post-AIA version are substantially the same, with only minor edits relating to joint inventorship issues and the addition of subsection markers.

IV. DAMAGES

143. Centripetal is entitled to damages adequate to compensate for infringement, "but in no event less than a reasonable royalty" for the making, using, offering for sale, selling, and importation into the United States of the Accused Products, together with interest and costs. 35 U.S.C. § 284; *see Trans-World Mfg. Corp. v. Al Nyman & Sons, Inc.*, 750 F.2d 1552, 1568 (Fed. Cir. 1984); *Siemens Medical Solutions USA, Inc. v. Saint-Gobain Ceramics & Plastics, Inc.*, 637 F.3d 1269, 1290-91 (Fed. Cir. 2011).

144. Centripetal must prove damages by a preponderance of the evidence. *SmithKline Diagnostics, Inc. v. Helena Lab'ys Corp.*, 926 F.2d 1161, 1164 (Fed. Cir. 1991). The damages analysis necessarily involves some "projection and inference." *See, e.g.*, *Kaufman v. Microsoft Corp.*, No. 16 Civ. 2880 (AKH), 2021 WL 242672, at *7 (S.D.N.Y. Jan. 25, 2021), *aff'd*, 34 F.4th 1360 (Fed. Cir. 2022) (denying motion for judgment as a matter of law and new trial because evidence of damages was sufficient to permit jury to make "reasonable inferences") (citing *Lindemann Maschinenfabrik, GmbH v. American Hoist & Derrick Co., Harris Press & Shear Div.*, 895 F.2d 1403, 1406 (Fed. Cir. 1990)). "When a 'reasonable royalty' is the measure, the amount may again [(as with lost profits)] be considered a factual inference from the evidence, yet there is room for exercise of a common-sense estimation of what the evidence shows would be a 'reasonable' award." *Lindemann Maschinenfabrik, GmbH*, 895 F.2d at 1406.

145. "[A] reasonable royalty is the minimum permissible measure of damages." *Deere & Co. v. Int'l Harvester Co.*, 710 F.2d 1551, 1558 n.9 (Fed. Cir. 1983). It is based on "the reasonable royalty . . . the [patentee] would have received through arms-length bargaining." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1324 (Fed. Cir. 2009).

146. The date of the hypothetical negotiation for the Asserted Patents is on or around June 20, 2017. *Georgia–Pacific Corp. v. U.S. Plywood Corp.*, 318 F.Supp. 1116, 1121 (S.D.N.Y. 1970); *Shield v. Inter Pool Cover Team*, 774 F.3d 766, 770 (Fed. Cir. 2014).

147. Centripetal's product practices the Asserted Claims of the Asserted Patents.

148. Centripetal marked its product with the Asserted Patents shortly after each issued.

149. Cisco had constructive notice of the '806, '193, and '176 Patents at least as of June 2017. 35 U.S.C. § 287(a); *see Global Traffic Techs. LLC v. Morgan*, 620 Fed. App'x 895, 906 (Fed. Cir. 2015) ("[M]arking the packaging . . . adequately served the purpose of providing constructive notice to the public that the entire Opitcom system was patented."); *LifeNet Health v. LifeCell Corp.*, 93 F. Supp. 3d 477, 508-09 (E.D. Va. 2015).

150. Cisco had actual notice of the '806, '193 and '176 Patents as of the date of the Complaint of February 13, 2018. 35 U.S.C. § 287(a). *See State Contracting & Engineering Corp. v. Condotte America, Inc.*, 346 F.3d 1057, 1073-74 (Fed. Cir. 2003)

151. Damages must be assessed on the footprint of the invention. *Uniloc USA, Inc. v. Microsoft Corp.*, 632 F.3d 1292, 1317 (Fed. Cir. 2011).

152. Apportionment can be done in various ways, including "by careful selection of the royalty base to reflect the value added by the patented feature, where that differentiation is possible; by adjustment of the royalty rate so as to discount the value of a product's non-patented features; or by a combination thereof." *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1226 (Fed. Cir. 2014). This flexibility is centered on "the difficulty that patentees may face in assigning value to a feature that may not have every been individually sold." *Virnetx, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1328 (Fed. Cir. 2014). The Federal Circuit has "never required

absolute precision in this task; on the contrary, it is well-understood that this process may involve some degree of approximation and uncertainty." *Id.*

153. Given the close comparability of the Keysight License (which applied the specified royalty rates to the entire revenue base), further apportionment is not required. "[W]hen a sufficiently comparable license is used as the basis for determining the appropriate royalty, further apportionment may not necessarily be required," because in such circumstances, apportionment is "built-in." *Vectura Ltd. v. GlaxoSmithKline LLC*, 981 F.3d 1030, 1040 (Fed. Cir. 2020) (affirming a reasonable royalty of 3% applied to total (unapportioned) infringing revenues, holding that apportionment was "built-in" through the use of a comparable license that likewise applied a royalty rate to an unapportioned revenue base); *Elbit Sys. Land & C4i Ltd. v. Hughes Network Sys., LLC*, 927 F.3d 1292, 1301 (Fed. Cir. 2019) (affirming damages award with built-in apportionment).

154. Apportionment reasonably reflecting the estimated value attributable to the infringing features of each Smallest Salable Patent Practicing Unit ("SSPPU") is based on consideration of the portion of the infringing functionality compared to the total functionality. *See Uniloc USA, Inc.*, 632 F.3d at 1317, *Finjan Inc. v. Blue Coat Sys.*, 879 F.3d 1299, 1312-13 (Fed. Cir. 2018) (approving "top level functions" methodology used here); *VirnetX, Inc..*, 767 F.3d at 1328 (precision not required).

155. Apportioning revenues based upon the top-level functions of the accused products is an appropriate methodology of apportionment for patent damages. *Blue Coat Sys.*, 879 F.3d at 1312-13 (approving "top level functions" methodology used here).

156. It is "improper to assume" that use of "a conventional element [in an invention] cannot be rendered more valuable," as all inventions use "earlier knowledge." *AstraZeneca AB v.*

Apotex Corp., 782 F.3d 1324, 1338-39 (Fed. Cir. 2015). "It is not the case that the value of all conventional elements must be subtracted from the value of the patented invention as a whole when assessing damages." *Id.*

157. Damages resulting from infringement of a system or computer readable media claim exists irrespective of the activation, configuration, execution, or use of the infringing technologies. *Secure Computing Corp.*, 626 F.3d at 1203-05; *VirnetX Inc. v. Apple Inc.*, 792 F. App'x 796 (Fed. Cir. 2019).

158. Because Cisco designed the Catalyst 9000 Switch, ISR/ASR Router, Firewall, and related software products to work together, and advertises and sells them as integrated systems, Cisco directly infringes the '806 and '176 Patents notwithstanding that customers must combine or assemble the components or activate embedded features. *Fantasy Sports Props., Inc.,* 287 F.3d at 1118 (finding direct infringement where users "must activate the functions" when "the user is only activating means that are already present in the underlying software."); *High Tech Med. Instrumentation, Inc*, 49 F.3d at 1556 ("if a device [here, an integrated system] is designed to be altered or assembled before operation, the manufacturer may be held liable for infringement if the device, as altered or assembled, infringes a valid patent."); *see also* Conclusions of Law Section II(A) (discussing direct infringement law in detail).

159. No such assembly or combination is required for Cisco's Catalyst 9000 Switch and ISR/ASR Router to directly infringe the '193 Patent.

160. The royalty base appropriately includes Cisco's foreign sales of the Accused Products because Cisco's foreign sales of the Accused Products are directly tied to Cisco's sale, manufacture, use and offers to sell the Accused Products in the United States under 35 U.S.C. § 271(a). *See, e.g., WesternGeco LLC v. ION Geophysical Corp.,* 138 S. Ct. 2129, 2138-39 (2018);

Plastronics Socket Partners, Ltd. v. Dong Weon Hwang, No. 2:18-cv-00014-JRG-RSP, 2019 WL 4392525, at *4-5 (E.D. Tex. June 11, 2019); *NTP, Inc.*, 418 F.3d at 1317 ("[t]he use of a claimed system under section 271(a) is the place at which the system as a whole is put into service, *i.e.* the place where control of the system is exercised and beneficial use of the system obtained"); *Uniloc USA, Inc. v. Microsoft Corp..*, 632 F. Supp. 2d 147, 155-56 (D.R.I. 2009); *Blue Spike, LLC v. Soundmouse Ltd*., No. 14 Civ. 2243 (CM), 2014 WL 6851259, at *4 (S.D.N.Y. Dec. 2, 2014).

161. The Keysight License is the most relevant license in the record as it is the only license to the Asserted Patents, and best available information to determine a reasonable royalty rate in this case. *ResQNet.com, Inc. v. Lansa, Inc.*, 594 F.3d 860, 872 (Fed. Cir. 2010) (permitting consideration of settlement license that was "the most reliable license in the record.").

162. The Keysight license is technically and economically comparable to a license resulting from a hypothetical negotiation between Centripetal and Cisco. *Id.*

163. The Keysight License should be considered in its proper context within the hypothetical negotiation framework to ensure that the reasonable royalty rate reflects "the economic demand for the claimed technology." *Id*. There is no error in relying on such evidence when the Court accounts for similarities and differences between past negotiations and the hypothetical negotiation. *See AstraZeneca AB*, 782 F.3d at 1335; *Vectura Ltd.*, 981 F.3d at 1040-41 (affirming damages award for infringement of single patent based on comparable license to 400 patents; *see also Elbit Sys. Land & C41 Ltd.* 927 F.3d at 1300 (collecting cases that show it is appropriate to rely on prior licenses, even in a settlement context, when they are sufficiently compared to the facts and circumstances of the case at issue); *Prism Techs. LLC v.*

Sprint Spectrum L.P., 849 F.3d 1360, 1372 (Fed. Cir. 2017) (no per se rule against use of settlement agreements).

164. *Georgia-Pacific* Factor Nos. 4, 5, 6, 8, 9, 10, and 11 warrant an upward influence on the royalty rate starting point found in the Keysight license. *Georgia–Pacific Corp. v. U.S. Plywood Corp.*, 318 F.Supp. 1116, 1121 (S.D.N.Y. 1970); *see also Aqua Shield*, 774 F.3d at 771-72 (with respect to Factor No. 8, infringer's actual profits are probative of anticipated profits at the hypothetical negotiation); *Lucent Techs, Inc.*, 580 F.3d at 1335 (noting that approximately 70-80% profit margin of the products at issue supports a higher versus lower reasonable royalty). *See Deere & Co.*, 710 F.2d at 1558 (with respect to Factor No. 9, company descriptions of the infringing products as having a "bright future" supported a higher royalty rate).

165. Centripetal is entitled to Royalty Rate of 8-10% on past damages between June 2017 and March 2023, and for the period of time from March 2023 to the date of payment, based on an accounting.

166. From June 20, 2017 through approximately March 23, 2023, the total apportioned royalty base calculated on worldwide revenues of all infringing products to the value of the inventions are [redacted]. PTX-1958 at Schedule 5. Applying the 8 and 10% royalty rate to this apportioned royalty base is $[redacted].

167. From June 20, 2017 through approximately March 23, 2023, the total apportioned royalty base calculated on U.S. revenues of all infringing products to the value of the inventions are [redacted]. PTX-1958 at Schedule 5.2. Applying the 8 and 10% royalty rate to this apportioned royalty base is [redacted].

168. Notwithstanding all the evidence, Cisco claimed there was insufficient proof that its products were sold in the infringing combinations. However, it never identified any credible

rebuttal evidence that the royalty base included non-infringing sales, such as the actual revenues of the purported infringing combinations even though Cisco is the only party with access to such information and was the only party that could obtain such information. The only evidence was that Cisco's revenues were for the infringing sales and Cisco did not present an opinion contrary to Centripetal's at trial, meaning that "any doubts about the amount" of damages are resolved "against the infringer." *DSU Medical Corp. v. JMS Co., Ltd.*, 471 F.3d 1293, 1309 (Fed. Cir. 2006); *Ryco, Inc. v. Ag-Bag Corp.*, 857 F.2d 1418, 1428 (Fed. Cir. 1988); *TWM Mfg. Co., Inc. v. Dura Corp.*, 789 F.2d 895, 900 (Fed. Cir. 1986) ("any adverse consequences must rest on the infringer when the inability to ascertain lost profits is due to the infringer's own failure to keep accurate or complete records."); *Lam, Inc. v. Johns-Manville Corp.*, 718 F.2d 1056, 1065 (Fed. Cir. 1983) ("[W]hen the amount of damages cannot be ascertained with precision, any doubts regarding the amount must be resolved against the infringer."); *see Kaufman Co., Inc. v. Lantech, Inc.*, 926 F.2d 1136, 1140–41 (Fed. Cir. 1991) ("Any doubts regarding the calculatory precision of the damage amount must be resolved against the infringer."); *Hartness Int'l Inc. v. Simplimatic Eng'g Co.*, 819 F.2d 1100, 1111 (Fed. Cir. 1987) ("[a]ny adverse consequences from Simplimatic's failure to keep accurate records must rest on Simplimatic."); *Paper Converting Machine Co.*, 745 F.2d at 22 ("[F]undamental principles of justice require us to throw the risk of any uncertainty upon the wrongdoer instead of upon the injured party."); *Sensonics, Inc. v. Aerosonic Corp.*, 81 F.3d 1566, 1572 (Fed. Cir. 1996) ("When the calculation of damages is impeded by incomplete records of the infringer, adverse inferences are appropriately drawn."). This rule dates back over a century from the simple proposition that any risk in estimating damages is based upon an uncertainty caused by defendant's own conduct, the defendant should bear the risk of uncertainty in quantifying damages from proven harm. *Story*

Parchment Co. v. Paterson Parchment Paper Co., 282 U.S. 555, 563 (1931) (labeling such a result a "perversion of fundamental principles of justice to deny all relief to the injured person, and thereby relieve the wrongdoer from making any amend for his acts. . . . The wrongdoer is not entitled to complain that they cannot be measured with the exactness and precision that would be possible if the case, which he alone is responsible for making, were otherwise . . . [T]he risk of the uncertainty should be thrown upon the wrongdoer instead of upon the injured party."). While most of these cases involve lost profits, the Court has applied them to lost profits with reasonable royalties. *TWM Mfg. Co., Inc.*, 789 F.2d at 900; *see Minco, Inc. v. Combustion Eng'g, Inc.*, 95 F.3d 1109, 1118 (Fed. Cir. 1996) (award included a component of lost profits and a reasonable royalty with doubts underlying the precise measurement of damages resolved against the infringer).

169. A damages model cannot reliably be apportioned or reduced from a royalty base without that base being based upon the SSPPU. *Commonwealth Scientific and Indus. Research Organisation v. Cisco Systems, Inc.*, 809 F.3d 1295, 1302 (Fed. Cir. 2015). Cisco's expert, Dr. Becker, did not apply the revenues for the SSPPU in his damages analysis, making his analysis unreliable. Specifically, Dr. Becker failed to include any revenue of the Catalyst 9000 Router, ISR/ASR Switch, and Firewall Product in his royalty base for his reasonable royalty opinion. For example, the accused products for the '193 Patent are the Catalyst 9000 Router and the ISR/ASR Switch and Dr. Becker did not include any revenue from these products in his royalty base and thus, Dr. Becker has no relevant or proper opinion for a reasonable royalty lump sum amount for the '193 Patent.

170. Noting the "tremendous" disparity between the parties' damages calculations, including in the royalty base, and Centripetal's unrebutted evidence, the Court gave Cisco

another opportunity after the close of all evidence to provide rebuttal evidence that its products were not sold as integrated systems and demonstrating "what [Cisco] considered to be the relevant products." Tr. 2970:23-2971:4, 2976:11-2977:17. It even invited Cisco to provide anything "you think would be helpful" because "you're not limited by what I ask for." Tr. 2976:11-2977:17. Despite this extraordinary request and having several weeks to comply, Cisco produced no supportive data.

171. Cisco also declined an opportunity for Dr. Becker to update his damages lump sum calculations as Centripetal did in preparation for the Rule 63 Hearing. As such, he has no relevant opinion on the applicable of the relevant royalty base for the relevant past damages period of June 2017 to March 2023. Additionally, he has no relevant opinion on an apportionment because his alleged use-based apportionment percentages do not reflect use over the relevant past damages period of June 2017 to March 2023.

172. Cisco failed to prove, pursuant to 28 U.S.C. § 1498, that any Accused Products were "used or manufactured" (i) "for" the U.S. Government; and (ii)"with the authorization or consent of" the U.S. government. *See IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359, 1361-62 (Fed. Cir. 2014). Cisco also failed to identify any specific government entities that it alleged satisfied the requirement under 1498.

173. The "'for the Government' prong of the definition" imposes "a requirement that the use or manufacture of a patented method or apparatus occur pursuant to a contract with the government and for the benefit of the government." *Sevenson Env't Servs. v. Shaw Env'tl*, 477 F.3d 1361, 1365-66 (Fed. Cir. 2007); *see id.* (Section 1498 not met where government "receives some benefit from the infringement" but the infringing use was not a "'governmental function' that the government sought or required"); *IRIS Corp.*, 769 F.3d at 1362 ("use is 'for the

Government' if it is 'in furtherance and fulfillment of a stated Government policy' which serves the Government's interests and which is 'for the Government's benefit.") (citation omitted).

174. Cisco must also prove that the government expressly or impliedly "authorized or consented to the manufacture of the allegedly infringing feature," such as in a government contract. *TecSec, Inc. v. Adobe Sys. Inc.*, 326 F. Supp. 3d 105, 112 (E.D. Va. 2018).

175. Cisco cannot establish its defense under 28 U.S.C. § 1498 by "produc[ing] extensive records of sales of its [Accused Products] to the government," rather, Cisco "needed to produce evidence during discovery that would show that [the Accused Products], particularly its allegedly infringing security feature, was manufactured for the government and that the government authorized or consented to the manufacturing of the device." *Id* at 111–12.

176. "Section 1498 does not shield the manufacturer or seller of an infringing item simply because it eventually ends up in the hands of the United States Government." 5 Donald S. Chisum, Chisum on Patents § 16.06 (2019); *see also, e.g., Systron-Donner Corp. v. Palomar Sci. Corp*, 239 F. Supp. 148, 149–51 (N.D. Cal. 1965) (defendant failed to show "use or manufacture" for the government with its "authorization and consent" under 28 U.S.C. § 1498 "even though some of the [infringing product] did eventually become property of the United States").Centripetal is entitled to prejudgment interest. Prejudgment interest should be granted under 35 U.S.C. § 284 based on the prime rate with interest accrued from the date the complaint was filed and compounded annually. *Sensonics, Inc.*, 81 F.3d at 1574 ("prejudgment interest is the rule, not the exception," and "prejudgment interest in patent cases is withheld only under exceptional circumstances"); *Gen. Motors Corp. v. Devex Corp.*, 461 U.S. 648, 656 (1983); *Nickson Indus., Inc. v. Rol Mfg. Co.*, 847 F.2d 795, 800 (Fed. Cir. 1988); *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 939 F.2d 1540, 1545 (Fed. Cir. 1991); *Lam, Inc.*, 718 F.2d at 1066;

Fresenius Med. Care Holdings, Inc. v. Baxter Int'l, Inc., No. C 03-1431 SBA, 2008 WL 928535, at *2 (N.D. Cal. Apr. 4, 2008).

177. Centripetal is entitled to post-judgment interest. 28 U.S.C. § 1961 ("Interest shall be allowed on any money judgment in a civil case recovered in a district court.") Post-judgment interest should be granted under 28 U.S.C. § 1961 on the entirety of the judgment using the "weekly average 1-year constant maturity Treasury yield . . . compounded annually" as mandated by 28 U.S.C. § 1961. *See Air Separation, Inc. v. Underwriters at Lloyd's of London*, 45 F.3d 288, 290-91 (9th Cir. 1995) ("[P]ostjudgment interest under 28 U.S.C. § 1961 applies to the prejudgment interest component of a monetary award.")*; Ivac Corp. v. Terumo Corp.*, No. 87-0413-B(M), 1990 WL 180201, at *2 (S.D. Cal. Aug. 8, 1990) (awarding prevailing patentee postjudgment interest on damages, fees, costs and prejudgment interest).

178. Centripetal is entitled to attorneys' fees based under 35 U.S.C. § 285, because a preponderance of the evidence shows that this is an exceptional case in terms of the substantive strength of Centripetal's litigating position, the unreasonable manner in which Cisco litigated this case, and the need under these circumstances to advance considerations of compensation and deterrence. *See Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 572 U.S. 545, 555-56 n.6 (2014); *Highmark Inc. v. Allcare Health Mgmt. Sys., Inc.*, 572 U.S. 559, 561-562 (2014). The determination that fees are warranted will be followed by an accounting to be submitted by Centripetal to determine the amount. *See Intex Recreation Corp. v. Team Worldwide Corp.*, 77 F. Supp. 3d 212, 217-18 (D.D.C. 2015) (finding case exceptional and fees warranted under 35 U.S.C. § 285 because defendant took "particularly weak" positions that "lacked factual support" and sought to re-litigate the court's claim construction).

179. Centripetal is entitled to all taxable costs incurred from the filing of the Complaint through the Court's decision at trial. "Unless a federal statute, these rules, or a court order provides otherwise, costs ... should be allowed to the prevailing party." Fed. R. Civ. P. 54(d)(1); *see* 28 U.S.C. § 1920 (listing the fees that may be taxed as costs); *Valador, Inc. v. HTC Corp.*, No. 16cv1162 (TSE/JFA), 2018 WL 4940721, at *12 (E.D. Va. May 30, 2018), *report and recommendation adopted sub nom. Valador, Inc.*, No. 1:16-CV-1162, 2018 WL 4937057 (E.D. Va. Oct. 10, 2018) (awarding costs for "obtaining transcripts, witness expenses, and fees for printing/reproduction and docket fees"). The prevailing party must provide a bill of costs that "distinctly set[s] forth each item thereof so that the nature of the charge can be readily understood," and the Clerk then taxes the costs, allowing "such items specified in the bill of costs as are properly chargeable as costs." E.D. Va. Loc. Civ. R. 54(D). The Court then reviews. *Id.* "By mandating that, subject to court intervention, costs be allowed to a prevailing party 'as of course,' the rule creates the presumption that costs are to be awarded to the prevailing party." *Cherry v. Champion Int'1 Corp.*, 186 F.3d 442, 446 (4th Cir. 1999) (citing *Delta Air Lines, Inc. v. August*, 450 U.S. 346, 352 (1981)). This presumption may only be overcome by the court "articulating some good reason for doing so." *Teague v. Bakker*, 35 F.3d 978, 996 (4th Cir. 1994) (quoting *Oak Hall Cap & Gown Co. v. Old Dominion Freight Line, Inc.*, 899 F.2d 291, 296 (4th Cir. 1990)).

V. WILLFUL INFRINGEMENT AND ENHANCEMENT OF DAMAGES

180. "The court may increase [any] damages up to three times the amount found or assessed." 35 U.S.C. § 284. Enhanced damages under this provision are warranted when the patent owner demonstrates by a preponderance of the evidence that a defendant willfully infringed the asserted patents, by knowing of the patent owner's patent and engaging in additional conduct evidencing deliberate or reckless disregard of the patent holder's patent

rights. *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 579 U.S. 93, 105-108 (2016); *see also Ironburg Inventions Ltd. v. Valve Corp.*, 64 F.4th 1274, 1296 (Fed. Cir. 2023) (affirming willful infringement based on reckless disregard of a patentee's known patent rights). The type of egregious conduct that warrants enhanced damages has been characterized as willful, wanton, malicious, bad-faith, deliberate, or consciously wrongful. *Halo Elecs., Inc.*, 579 U.S. at 103-105.

181. The existence or presentation of a reasonable defense to infringement or validity is insufficient to absolve the infringer of willful infringement. *Id.*. at 105-108.

182. Cisco willfully infringed the Asserted Patents because it intentionally and in bad faith chose to copy Centripetal's patented technology which Centripetal had presented to Cisco and which Cisco knew to be patented, with reckless disregard for Centripetal's property rights.

183. Cisco knew of the '806 Patent as early as February 2016. *See* Findings of Fact, Sections VIII(J), IX(A). Cisco also knew of Centripetal's patent-practicing RuleGATE product and had received multiple demonstrations. Despite Cisco's knowledge, Cisco released the Catalyst 9000 Switch with DNA, ISR/ASR Router with DNA, and Firewall with FMC. *See, e.g.*, *WBIP, LLC*, 829 F.3d at 1342 (defendant's awareness of plaintiff's patented and marked product, as well as defendant's pre-suit knowledge of at least one patent, constituted willful infringement).

184. Cisco and Centripetal had multiple meetings and discussions about Centripetal's patented technology prior to the release of Cisco's infringing functionalities, further supporting that Cisco's infringement is willful. *See* Findings of Fact, Section II(C); *see, e.g.*, *Georgetown Rail Equip. Co. v. Holland L.P.*, 867 F.3d 1229, 1245 (Fed. Cir. 2017) (substantial evidence supported willful infringement based on, *inter alia*, prior business dealings and circumstantial evidence of copying).

185. At a minimum, Cisco willfully infringed the Asserted Patents because it "acted despite a risk of infringement that was "either known or so obvious that it should have been known to [Cisco]." *Arctic Cat Inc. v. Bombardier Recreational Prod. Inc.*, 876 F.3d 1350, 1371 (Fed. Cir. 2017) (internal citations and quotation marks omitted).

186. Given Cisco's willful infringement, among other factors, it is appropriate to award enhanced damages. Courts are guided by the *Read* factors in determining the availability and amount of enhanced damages, but the award is ultimately within their discretion. *See Georgetown Rail Equip. Co.*, 867 F.3d at 1244 (citing *Read Corp. v. Portec, Inc.*, 970 F.2d 816, 826-27 (Fed. Cir. 1992)). Those factors include:

- whether defendant "deliberately copied the ideas or design of another," where "'[i]deas' and 'design' would encompass, for example, copying the commercial embodiment, not merely the elements of a patent claim;"
- whether defendant "investigated the scope of the patent and formed a good-faith belief that it was invalid or that it was not infringed" once it had learned of the patent;
- defendant's litigation conduct;
- defendant's size and financial condition;
- whether the issues presented a close case;
- the duration of defendant's misconduct;
- whether defendant took any remedial actions;
- defendant's motivation for harm; and
- any attempts that defendant made to conceal its misconduct.

Read Corp., 970 F.2d at 826-27, n.7.

187. No individual *Read* factor is required to support a finding that enhanced damages are appropriate. *SRI Int'l, Inc. v. Advanced Tech. Labs., Inc.*, 127 F.3d 1462, 1469 (Fed. Cir. 1997).

188. Cisco was aware of Centripetal's patents, including the '806 Patent and various pending applications, well before this suit was filed. It received multiple demonstrations of Centripetal's patent-practicing, marked product, which is of course a "commercial embodiment" of Centripetal's patent claims. Despite knowing of Centripetal's patent protection—indeed, despite its employee advising that Cisco should internally "study their claims"—Cisco proceeded to willfully infringe. Cisco attempted to conceal its copying by acting as if it would like to partner with or invest in Centripetal. *See* Findings of Fact, Sections II(C)-(D), IX(A).

189. Cisco presented no evidence that it formed a good-faith belief that it did not infringe or that the Asserted Patents were invalid prior to this suit. Moreover, the inconsistencies and lack of credibility in the defenses that Cisco presented in this litigation demonstrate that, despite its allegations, Cisco does not have a good-faith belief in non-infringement or invalidity to this day. *See* Findings of Fact, Sections V, VI, and VII, VIII(J), and IX(A).

190. Cisco is a huge and long-established company with many successful product offerings and a global footprint. Cisco's business can easily tolerate even treble damages. *See* Findings of Fact, Section II(B).

191. Cisco's misconduct has continued unchecked for years, and Cisco has presented no evidence of remediation. *See* Findings of Fact, Section IX(A)-(C).

192. Cisco has engaged in exceptional and unacceptable litigation tactics. For example, despite the Court's repeatedly expressed concerns over delay, Cisco dragged this case out over 7 years and sought to piecemeal the issues up to the very end. It also sought to confuse

and mislead in its presentation of evidence in this case, and to belatedly pad the record with documents multiple times. *See* Findings of Fact, Section IX(C); *see also, e.g.*, *SRI Int'l, Inc., v. Cisco Sys., Inc.*, 14 F.4th 1323, 1328-29 (Fed. Cir. 2021) (evidence that Cisco's defenses were unreasonable—including that Cisco misrepresented how its accused products work, as shown by "Cisco's own technical witness"—supported a finding of willful infringement and enhanced damages).

VI. INJUNCTIVE RELIEF

193. Centripetal is entitled to a narrowly-tailored injunction on the manufacture, use, sales, offer for sale, and importation in the United States of Cisco's Firewalls. *See eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006).

194. A permanent injunction is warranted where a plaintiff has demonstrated "(1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." *eBay Inc.,* 547 U.S. at 391.

195. Centripetal has suffered irreparable injury from the infringing conduct of its direct competitor, Cisco, as Centripetal is "being forced to compete against products that incorporate and infringe its own patented inventions" and the "patented feature is one of several features that cause consumers to make their purchasing decisions." *Apple Inc. v. Samsung Elecs. Co., Ltd.*, 809 F.3d 633, 641-42 (Fed. Cir. 2015); *see* Findings of Fact, Section VIII(C). An equitable remedy is appropriate given this competition, particularly since Cisco is a far larger company with a diverse product offering, while Centripetal's patented technology is its "flagship" market offering. *See, e.g.*, *Acumed LLC v. Stryker Corp.*, 551 F.3d 1323, 1327 (Fed. Cir. 2008). In such circumstances, an injunction is appropriate. *Id.*

196. Centripetal has also suffered injury to its reputation. *See* Findings of Fact, Section X. "[P]ast harm to a patentee's market share, revenues, and brand recognition is relevant to determining whether the patentee has suffered an irreparable injury." *02 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.,* 449 F. App'x 923, 932 (Fed. Cir. 2011) (internal quotation omitted).

197. These harms are difficult to quantify particularly given the fact that Cisco is a much larger competitor. *See i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 862 (Fed. Cir. 2010).

198. There is also prospective irreparable harm in the absence of an injunction. For example, would-be infringers would be encouraged to try to gain market access and opportunities via infringing Centripetal's patents, which could result in "significant litigation expenses and uncertainty about the value of Centripetal's patents." *Amgen, Inc. v. F. Hoffman-La Roche, Ltd.*, 581 F. Supp. 2d 160, 212 (D. Mass. 2008), *vacated in part on different grounds*, 580 F.3d 1340 (Fed. Cir. 2009).

199. The Keysight License does not militate against an injunction, because Centripetal entered into it only in the context of enforcing its patent rights in litigation and generally does not license its technology in the ordinary course of business. *See 02 Micro*, 449 F. App'x at 933; *Acumed LLC*, 551 F.3d at 1328 ("A plaintiff's past willingness to license its patent is not sufficient per se to establish lack of irreparable harm if a new infringer were licensed.") (internal citation omitted).

200. The public interest would not be disserved by an injunction because Centripetal has a scalable business model and can meet the demand for the infringing security technologies

in the enjoined Firewalls. *See* Findings of Fact, Section X. Cisco also did not present evidence of any public interest that would be harmed by injunctive relief.

VII. CREDIBILITY DETERMINATIONS

201. "Credibility determinations are within the province of the trier of fact and are not reviewable on appeal.'" *United States v. Magwood*, 528 F. App'x 331, 332 (4th Cir. 2013) (citations omitted). "[A]t a bench trial, the judge sits as finder of fact and is empowered to evaluate the evidence, determine the credibility of witnesses, and draw whatever reasonable inferences the judge deems appropriate given his factual findings." *See also Weisner v. Liberty Life Assurance Co. of Bos.*, 192 F. Supp. 3d 601, 608 (D. Md. 2016). Cisco has conceded that the Court can determine the credibility based on the record, and the 4th Circuit has acknowledged that "contradicted testimony" and "conflicting responses on direct and cross-examination undoubtedly undermined [a witness's] credibility." *United States v. Burgos*, 94 F.3d 849, 867 (4th Cir. 1996).

A. Credibility Determinations for the '193 Patent

202. Dr. Mitzenmacher is credible for the '193 Patent as he relied upon twenty-two (22) trial exhibits, including confidential technical documents, Cisco's witness testimony, and source code, for the new Catalyst 9000 Switch and ISR/ASR Router technology that was launched in June 2017. *See* PTX-175, PTX-242, PTX-563, PTX-576, PTX-992, PTX-995, PTX-1226, PTX-1260, PTX-1262, PTX-1276, PTX-1280, PTX-1281, PTX-1288, PTX-1303, PTX-1313, PTX-1356, PTX-1409, PTX-1849, PTX-1911, PTX-1912, PTX-1913, and PTX-1914.

203. Cisco's technical expert for the '193 Patent, Dr. Crovella, took positions that established that his testimony was not credible or supported.

204. In support of his opinion, Dr. Crovella did not cite any technical Cisco document produced that post-dated June 20, 2017. Instead, he relied on ex post facto animations which

were created for the litigation, and do not accurately portray the current functionality of the accused products. *See* Findings of Fact, Section V(C).

205. Cisco did not call any witness who authored any of the Cisco technical documents relied upon by Centripetal in their infringement case, further undermining any credibility of Dr. Crovella. See Findings of Fact, Section V(C).

206. Dr. Crovella relied on a 41 page PowerPoint presentation created for the litigation to support his opinion of noninfringement of the '193 Patent asserted claims at trial. See Findings of Fact, Section V(C).

207. As purported evidence for his opinion, Dr. Crovella only referred to one Cisco technical document, PTX-1276, dated 2014, during his entire noninfringement trial testimony. See Findings of Fact, Section V(C).

208. Dr. Crovella did not point to any Cisco trial exhibit concerning the new Catalyst 9000 Switch or ISR/ASR Router that was launched in 2017, which were the products at issue. Indeed, for much of his testimony, he provided testimony describing why Stealthwatch did not infringe the '193 Patent, but Stealthwatch was not accused of infringing the '193 Patent. See Findings of Fact, Section V(C).

209. During cross-examination, Dr. Crovella's lack of credibility was established because he admitted that the Catalyst 9000 Switches and ISR/ASR Routers would block some communication between networks but allow others, undermining his own non-infringement position. See Findings of Fact, Section V(C).

210. Dr. Crovella's lack of credibility was established because he applied different claim constructions for purposes of invalidity and non-infringement. See Findings of Fact, Section V(C).

211. Dr. Crovella's lack of credibility was established by the Court's calling into question the veracity of Dr. Crovella's PowerPoint slides. See Findings of Fact, Section V(C).

B. Credibility Determinations for the '806 Patent

212. The credibility of Centripetal's technical expert, Dr. Mitzenmacher, is established for the '806 Patent as he relied upon twenty-six (26) trial exhibits, including confidential technical documents, Cisco's witness testimony, and source code, for the new Catalyst 9000 Switch, ISR/ASR Router and DNA Center technology, and Cisco's Firewalls with FMC. See PTX-244, PTX-408, PTX-992, PTX-1195, PTX-1196, PTX-1241, PTX-1263, PTX-1277, PTX-1288, PTX-1289, PTX-1291, PTX-1293, PTX-1294, PTX-1303, PTX-1313, PTX-1315, PTX-1348, PTX-1385, PTX-1390, PTX-1393, PTX-1849, PTX-1915, PTX-1916, PTX-1917, PTX-1918, and PTX-1920.

213. Cisco's technical expert for the '806 Patent, Dr. Reddy, took positions that established that his testimony was not credible or supported.

214. Dr. Reddy relied on a PowerPoint presentation created for the litigation to support his opinion of noninfringement of the '806 Patent. See Findings of Fact, Section VI(C).

215. During Dr. Reddy's entire noninfringement trial testimony, he referred to just one Cisco technical document, PTX-1390. See Findings of Fact, Section VI(C).

216. Dr. Reddy lacked of credibility as his animations created for the litigation contradicted Cisco's own documents, and the Court called Dr. Reddy out on the contradiction. See Findings of Fact, Section VI(C).

217. Dr. Reddy's lack of credibility was established when he testified that rules were not applied on the ingress and egress of packets in the Catalyst 9000 Switches or ISR/ASR Routers, which was contradicted by the testimony of Cisco's engineer, Mr. Jones (*see, e.g.*, Tr.

2543:9-11, 2561:25-2562:1, 2571:12-2573:8) and Cisco's actual business records, as opposed to litigation-created demonstratives. See Findings of Fact, Section VI(C).

218. Dr. Reddy lacked credibility as he created a demonstrative animation that conflicted with Cisco's technical documents and engineers and he opined that rules were only applied by the products for packets entering ("ingress") the product and not when exiting ("egress") the product. In actuality, all evidence showed that rules were applied both at the ingress and egress. See Findings of Fact, Section VI(C).

219. Dr. Reddy lacked of credibility as he testified that he applied different claim interpretations for his invalidity versus non-infringement opinions for the '806 Patent. See Findings of Fact, Section VI(C).

C. Credibility Determinations for the '176 Patent

220. The credibility of Centripetal's technical expert, Dr. Cole, is established as he relied on fifteen (15) trial exhibits based, including confidential technical documents, Cisco's witness testimony, and source code, for the new Catalyst 9000 Switch, ISR/ASR Router and Stealthwatch technology. See PTX-134, PTX-408, PTX-547, PTX-569, PTX-572, PTX-591, PTX-595, PTX-1009, PTX-1018, PTX-1046, PTX-1060, PTX-1065, PTX-1089, PTX-1849, and PTX-1930. See Findings of Fact, Section VII(C).

221. Cisco's technical expert for the '176 Patent, Dr. Almeroth, took positions that established that his testimony was not credible.

222. Dr. Almeroth lacked credibility as he relied on a PowerPoint presentation created for the litigation to support his opinion of noninfringement of the '176 Patent. During cross examination, Dr. Almeroth admitted that his slide that he relied on to show how the accused system operates (slide 22) was not based on any Cisco technical document, but instead was created for this litigation. See Findings of Fact, Section VII(C).

223. Dr. Almeroth's lack of credibility was established when he admitted during cross examination that he made erroneous statements. During his entire noninfringement trial testimony, he refers to a few trial exhibits that Dr. Cole introduced, and proceeds to testify that Dr. Cole got it incorrect. Dr. Almeroth opined that Dr. Cole's infringement opinion relied on the systems' use of logs provided by Cisco's proprietary logging technology, NetFlow, as the logs outlined by the claim language. Dr. Almeroth construed the claims to require identification and generation of logs out of the same network device on ingress and egress. Therefore, Dr. Almeroth averred that the Cisco system cannot infringe, because in his opinion, the Catalyst 9000 Switches and ISR/ASR Routers do not generate NetFlow on both ingress into a device and egress out of one network device. However, on cross examination, Dr. Almeroth conceded that his single device construction is incorrect. Moreover, Cisco's technical documents refute Dr. Almeroth's conclusion. PTX-1060, a Cisco technical document dated December of 2017, shows that the Catalyst switches have the ability to export NetFlow on ingress and egress. Dr. Almeroth, on cross-examination, even admitted that the Catalyst 9000 Switches and ISR/ASR Routers can be configured to export ingress and egress NetFlow. See Findings of Fact, Section VII(C).

224. Dr. Almeroth's lack of credibility was established when, on cross examination, he confirmed that NetFlow can be configured on ingress and egress, which is an admission that contradicted his previous testimony. With this admission, he shifted the crux of his noninfringement opinion to be that Stealthwatch produces an error based on producing both types of NetFlow. To support that claim, Dr. Almeroth relied solely on the presentation of source code from the 6.5.4 version of Stealthwatch that operated without enhanced NetFlow or the integration of Cognitive Threat Analytics (CTA). He cited to no technical document that

confirms that the accused current version of Stealthwatch produces an error when exporting both ingress and egress NetFlow. In fact, the technical release notes for CTA, which was incorporated into Stealthwatch in 2018, support that CTA produced the ability for the correlation of NetFlow telemetry. See Findings of Fact, Section VII(C).

225. Dr. Almeroth's lack of credibility was established because he admitted he used a different understanding of the asserted claims of the '176 Patent for his Invalidity Opinion than for his Non-Infringement Opinion. He also testified that while the claims would be valid if he applied the same interpretation used for infringement for validity, he was "not offering opinions [for validity] under what [he] believe[s] is the proper claim scope." See Findings of Fact, Section VII(C).

226. Dr. Almeroth ignored that rules being generated in response to correlation was a new feature that was not previously included in Stealthwatch and Cisco's technical documents contradict his testimony. See Findings of Fact, Section VII(C).

D. Credibility Determinations on Damages

227. Cisco's expert for damages, Dr. Becker, took positions that established that his testimony was not credible.

228. Dr. Becker's lack of credibility was established when he claimed that the reasonable royalty for the '193, '806, and '176 Patents was $934,323 because the accused functionality was allegedly of minimal value. However, this is contradicted by the fact that Cisco offers for sale and sells the Accused Products as integrated systems that provide network security functionality "of critical importance" to Cisco and its customers. Cisco markets and sells its products as a "cybersecurity architecture" and "as one product" based on Cisco's SEC statements, presentations, and technical marketing materials. Cisco's technical expert, Dr.

Schmidt, confirmed that customers need Cisco's "comprehensive technique" and "[c]omprehensive set of products." *See* Findings of Fact, Section VIII(L).

229. Additionally, Dr. Becker's lack of credibility was established because, despite the overwhelming evidence, as described above, Cisco contended that there was insufficient proof that its products were sold in the infringing combinations. As a result, Dr. Becker excluded entirely from his proposed royalty base all revenues from the Catalyst 9000 Switch, ISR/ASR Router, and the Firewall Product, which are the SSPPU. Despite an unlimited additional opportunity to support its claim that all revenues for the Accused Products were not sold as part of infringing combinations, Cisco was unable to produce any data supporting Dr. Becker's claim or analysis. *See* Findings of Fact, Section VIII(L).

230. Dr. Becker's lack of credibility was established by the fact that his damages figure is objectively unreasonable and the product of unreliable methodology for various additional reasons. For example, Dr. Becker's damages figure is less than the $3.86 million that Cisco stated was the cost of a ***single*** data breach. As another example, Dr. Becker's damages figure is also objectively unreasonable because it makes the effective royalty rate an infinitesimal fraction, which does not reflect a reasonable royalty that parties at a hypothetical negotiation would agree upon. Additionally, Dr. Becker's damages figure is far lower than the agreed-upon rate from the Keysight License, highlighting its unreasonableness. Further, Dr. Becker's damages figure is also unreasonably low because it is inconsistent with Cisco's acknowledgement that security was "the top IT priority for many of our customers," (Tr. 1451:12-1452:6; *see also* Tr. 1453:13-1454:24 (discussing PTX-560 at 771)), such that Cisco would in fact find Centripetal's patented security solutions very valuable. Moreover, Dr. Becker's damages figure is unreasonably low because it is inconsistent with Cisco's

representation that it was unaware of any other licenses relevant to the technology of the Asserted Patents, which reinforces that no one was doing anything close to Centripetal's technology. This exclusivity justifies a higher value at the hypothetical negotiation. *See* Findings of Fact, Section VIII(L).

231. Dr. Becker's lack of credibility was established by his contention that the Accused Products are not marketed and sold as integrated systems, which conflicted with Dr. Schmidt's testimony that "only those customers [that] are extremely looking forward to having their networks hacked" would fail to use Cisco's "comprehensive set of products." See Findings of Fact, Section VIII(L).

232. Dr. Becker's lack of credibility was established by the fact that his apportionment position was also unreasonable and unreliable. For example, Dr. Becker claimed to apportion "by a percentage of how many [security] alerts there were as compared to how many packets were checked." Dr. Becker also plucked that percentage (0.4%) from Mr. Scheck's testimony about what proportion of CTA-identified threats are addressed by Stealthwatch and used it to reach his extremely low damages figure. However, Cisco offered no support for Dr. Becker's "huge reduction" based on the percentage of identified alerts. See Findings of Fact, Section VIII(L).

233. Dr. Becker's lack of credibility was established when the Court noted that Dr. Becker's apportionment theory "borders on the absurd" and that "[t]here's no way the Court will accept that analysis." See Findings of Fact, Section VIII(L).

234. Dr. Becker's lack of credibility was established when he adopted an apportionment position that was also objectively unreasonable and unreliable because it was akin

to arguing that airbags and seat belts are of no value unless deployed in an emergency. See Findings of Fact, Section VIII(L).

235. Dr. Becker's lack credibility was established by his analysis that the routers and switches were not the real source of the patented improvement, such that their revenues are not part of the royalty base, because it conflicted with the testimony of Cisco's engineers, Messrs. Llewallyn and Jones. For example, Mr. Llewallyn confirmed that the Catalyst 9000 Switch and ISR/ASR Router can quarantine malicious traffic in response to information from Stealthwatch. The switches and routers are thus an integral part of the patented solutions and essential to delivering the benefits of the Asserted Patents to Cisco's customers. See Findings of Fact, Section VIII(L).

236. Dr. Becker's lack of credibility was also established by his failure to update his opinion to have a relevant or applicable opinion for his reasonable royalty analysis to account for the increased damages period from 2017 to 2023 when Cisco updated its revenues, establishing that his opinion should thus be disregarded. See Findings of Fact, Section VIII(L).

E. Credibility Determinations on Willfulness

237. Centripetal presented three credible witnesses related to willfulness, two fact witnesses (Steven Rogers and Johnathan Rogers) and one expert witness (Dr. Eric Cole) to testify about the parties' interactions prior to this litigation. See Findings of Fact, Section IX(B).

238. Steven Rogers credibly testified about Cisco's first contact with Centripetal in 2015 when he was personally contacted by Pavan Reddy to learn about Centripetal's patented technology, which it viewed as a solution that "fit into the types of solutions [Cisco] needed for customers . . . that went beyond the offerings that Cisco had at the time." Mr. Reddy and Mr. Rogers had a follow-up meeting that same year, where Centripetal provided a demonstration of

its system and explained why it was an effective method of cyber defense. This testimony was unchallenged by Cisco, showing that it was credible. See Findings of Fact, Section IX(B).

239. Mr. Rogers also credibly provided testimony that as a result of these meetings, on January 26, 2016, Centripetal and Cisco entered into a nondisclosure agreement ("NDA"). This testimony was unchallenged by Cisco, showing that it was credible. See Findings of Fact, Section IX(B).

240. Mr. Rogers credibly testified that after Centripetal and Cisco executed the NDA, the parties had another meeting in February 2016. His credibility on this was established through PTX-547, a contemporaneous document dated at the time of the February meeting, was marked and Mr. Rogers testified that he "believe[d] it's the presentation that was provided to Cisco." Referring to page 7 of PTX-547, Mr. Rogers testified that Cisco was provided information about Centripetal's patented filter algorithms and that the system was patented. See Findings of Fact, Section IX(B).

241. Jonathan Rogers credibly testified and confirmed Centripetal's meeting with and demonstration to Cisco in 2015. Mr. Rogers also proved testimony regarding entering into an NDA with Cisco in early 2016, and the dated NDA was marked as PTX-99. See Findings of Fact, Section IX(B).

242. Mr. Rogers testimony was credible because it provided detailed testimony supported by contemporaneous documents (PTX-547 and PTX-102), about the February 4, 2016, meeting where Centripetal presented information about its patented technology and products to Cisco in a WebEx meeting, including details of its patented technology for the Asserted Patents. For example, Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies

'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics." Mr. Rogers testified that during that meeting, Centripetal presented "detailed, highly sensitive, confidential and proprietary information about its patented technology and products," including its patented filter algorithms to prevent exfiltration ('193 Patent), correlation algorithms ('176 Patent), and rule swapping ('806 Patent). Mr. Rogers also credibly testified how Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation technologies 'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics." Centripetal also answered various questions about its patented technologies at the meeting. See Findings of Fact, Section IX(B).

243. Mr. Rogers's testimony was credible because Cisco did not undispute that Centripetal and Cisco had further follow-up meetings and communications after the February 2016 WebEx meeting, demonstrating Cisco's continued interest in Centripetal. For example, in July 2016, Cisco invited Centripetal to be a technology partner at its Cisco Live conference, where Centripetal again presented its patented solution. In December 2016, Oppenheimer presented to Cisco additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGATE functionalities covered by the Asserted Patents. *See* Findings of Fact, Section II(C), IX(A)-(B).

244. For every fact about Centripetal's interactions with cisco that Steven Rogers and Jonathan Rogers testified to at trial, there were a number of contemporaneous documents to support their trial testimony, establishing their credibility. *See* Findings of Fact, Section IX(B).

245. Dr. Cole provided credible and unrebutted expert insight and opinions into these types of interactions from one skilled in the art. *See* Findings of Fact, Section IX(B).

246. Cisco presented two fact witnesses at trial that attempted to recharacterize the contemporaneous exhibits regarding Centripetal's and Cisco's meetings – Timothy (TK) Keanini and Karthik Subramanian. Neither of these two witnesses was credible on the circumstances of the meeting, because their testimony was inconsistent with contemporaneous documents. *See* Findings of Fact, Section IX(B).

247. Mr. Keanini was put on the stand to explain his February 5, 2016, email the day after the WebEx meeting with Centripetal. He wrote an internal email to his team stating:

> It appears that most of their **intellectual property** lays in the claim that given 'n' amount of signatures (they call them rules) they are able to instrument them in an inline device. . . . What might be work [sic] **exploration is to look at these algorithms** they have and how general purpose they may be for data synthesis – high performance set theoretical functions. Again, **knowing what patent offices will allow and not allow**, I'd be very surprised if they were able to make claims on the algorithms themselves but **we don't know until we study their claims**.

See Findings of Fact, Section IX(B).

248. During cross examination, Mr. Keanini testified that he had no memory of Centripetal talking about their patents at the meeting. When shown page 7 of the meeting presentation marked PTX-547 that discussed Centripetal's patents, he changed his testimony and said they only discussed their patents at a high level. See Findings of Fact, Section IX(B).

249. When asked about the first sentence of his email marked as PTX-90 about intellectual property, he responded as follows:

> Q. So when you're talking about intellectual property you're talking about patents, right?
>
> A. No. Again, I may have chosen the wrong word here. I was just -- in that first paragraph I was just trying to establish that I was paying attention at the meeting and that I understood what they

> did. I didn't really mean their intellectual property. I meant the stuff they said they did in that demo.

See Findings of Fact, Section IX(B).

250. When asked about the second sentence where it stated it might be worth exploring Centripetal's algorithms, Mr. Keanini testified Centripetal "didn't really talk about their algorithms." See Findings of Fact, Section IX(B).

251. When asked about his statement about the patent office and studying Centripetal's claims, Mr. Keanini testified that he "was just trying to express the fact that I wasn't -- I didn't want to come off as arrogant." See Findings of Fact, Section IX(B).

252. Cisco also presented Mr. Karthik Subramanian to testify about the February 2016 meeting between Centripetal and Cisco. His testimony was not credible because during his deposition in this case, he had no memory of Centripetal or any meeting with Centripetal. At trial, he said he had his memory refreshed by the documents and provided testimony about the documents. However, even at trial he could not remember if he actually attended the February 2016 meeting.

> Q. And you said you don't recall going to the February 4th meeting one way or the other. You may have gone, you just don't recall, correct?
>
> A. Yes. You know, I don't recall the specifics of that, you know. It was organized by my team. I think more than likely I was part of that meeting as well, I just don't remember specifics.

Mr. Subramanian was pure speculation and was not credible. See Findings of Fact, Section IX(B).

Respectfully submitted,

Dated: June 9, 2023

By: */s/ Stephen E. Noona*

Stephen Edward Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre
Lisa Kobialka
James Hannah
Hannah Lee
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
hlee@kramerlevin.com

Cristina L. Martinez (pro hac vice)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Telephone: (212) 715-9000
Facsimile: (212) 715-8000
cmartinez@kramerlevin.com

ATTORNEYS FOR PLAINTIFF
CENTRIPETAL NETWORKS, LLC

CERTIFICATE OF SERVICE

I hereby certify that on June 9, 2023, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to counsel of record.

/s/ Stephen E. Noona
Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com